PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-055242
(43)Date of publication of application : 26.02.1999

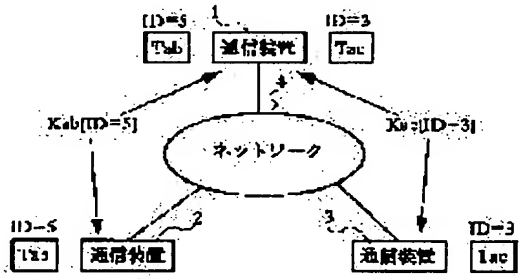
(51)Int.Cl. H04L 9/08

(21)Application number : 09-208198
(22)Date of filing : 01.08.1997

(71)Applicant : HITACHI LTD
(72)Inventor : OURA TETSUO
SHIN YOSHIFUMI

(54) CRYPTOGRAPHIC KEY UPDATING METHOD AND STORAGE MEDIUM RECORDING CRYPTOGRAPHIC KEY UPDATE PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To reduce the load on a device manager and to change a cryptographic key without interrupting communication by permitting a first communication equipment to select an identifier from a cryptographic key table, informing a second communication equipment of it, permitting the second communication equipment to take out the key corresponding to the identifier from the cryptographic key table.
SOLUTION: The cryptographic key tables where the plural cryptographic keys are registered for respective opposite parties executing cryptographic communication are set in the respective communication equipments 1-3. The cryptographic key tables Tab and Tac for executing cryptographic communication with the communication equipments 2 and 3 are provided for the communication equipment 1. The cryptographic tables Tab and Tac for executing cryptographic communication with the communication equipment 1 are set in the communication equipments 2 and 3. For using the key of ID=5 in the cryptographic communication between the communication equipment 1 and the communication equipment 2, ID=5 is set as an initial value. In the respective equipments, one cryptographic key is taken out from the cryptographic key table based on ID and it is used for the ciphering of data to be transmitted and the decoding of received data so as to execute cryptographic communication.



LEGAL STATUS

[Date of request for examination] 31.08.2000
[Date of sending the examiner's decision of rejection] 06.04.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] It is the updating approach of a cryptographic key used in case two or more communication devices are connected in a network and cryptocommunication is performed among said two or more communication devices. The cryptographic key table which consisted of identifiers which specify two or more cryptographic key and each cryptographic key in the communication device which performs said cryptocommunication is created. The 1st communication device of said communication devices which perform cryptocommunication chooses the identifier from said cryptographic key table. The renewal approach of a cryptographic key characterized by said 2nd communication device with which the identifier was notified to the 2nd communication device of the communication devices which perform said cryptocommunication, and said the 1st communication device and identifier were notified taking out the cryptographic key corresponding to an identifier from said cryptographic key table.
[Claim 2] It is the updating approach of a cryptographic key used in case two or more communication devices are connected in a network and cryptocommunication is performed among said two or more communication devices. The communication device which performs said cryptocommunication holds the same master key, respectively, and the 1st communication device of said communication devices which perform cryptocommunication generates a hash key. It is the renewal approach of a cryptographic key about it being characterized by considering as the cryptographic key which updated the result to which said hash key was notified to the 2nd communication device of the communication devices which perform said cryptocommunication, and said the 1st communication device and said 2nd communication device hashed said master key with said hash key.
[Claim 3] It is the updating approach of a cryptographic key used in case two or more communication devices are connected in a network and cryptocommunication is performed among said two or more communication devices. The cryptographic key master table which consisted of identifiers which specify two or more cryptographic key and each cryptographic key in the communication device which performs said cryptocommunication is created. The 1st communication device of the communication devices which perform said cryptocommunication chooses one identifier from said cryptographic key master table. The identifier is notified to the 2nd communication device of the communication devices which perform said cryptocommunication. Said 1st communication device which performs cryptocommunication generates a hash key, and notifies the generated hash key to said 2nd communication device. The renewal approach of a cryptographic key characterized by considering as the cryptographic key which updated the result to which said the 1st communication device and said 2nd communication device took out the cryptographic key corresponding to said selected identifier from said cryptographic key master table, and hashed said cryptographic key with said hash key.
[Claim 4] It is the storage which records the program which updates the cryptographic key used in case cryptocommunication is performed among two or more communication devices connected in the network. Said program The step which creates the cryptographic key table which records correspondence with the identifier for specifying two or more cryptographic key and each cryptographic key in the communication device which performs cryptocommunication, The step which chooses the identifier corresponding to one cryptographic key in said two or more cryptographic keys, and this cryptographic key from said code table in case the communication device which performs cryptocommunication transmits data, The storage characterized by consisting of a step which notifies said selected identifier to the communication device of

a data transmission place, and a step which takes out the cryptographic key to which this identifier corresponds from said cryptographic key table according to reception of said identifier notified by cryptocommunication from other communication devices.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention is applied to renewal of the cryptographic key especially used at the time of the cryptocommunication between communication devices about the storage which recorded the renewal approach of a cryptographic key, and the renewal program of a cryptographic key, and relates to an effective technique.
[0002]
[Description of the Prior Art] According to the place which this invention person examined, for example between the communication devices with which cryptocommunication is performed in the system by which network connection of the communication devices, such as a personal computer, was carried out, the encryption key used in the case of the data encryption which communicates mutually, and a decryption is shared, and cryptocommunication is performed by using the cryptographic key.
[0003] In addition, as an example to which the encryption communication technology of this kind of network is stated in detail, they are July 30, 1996, Ohm-Sha Issue, and D.Brent. Chapman, Elizabeth There are D.Zwicky (work) and "fire wall construction Internet SEKYURITE" P393, and distribution of the key of the network level encryption in the Internet is indicated by this reference.
[0004]
[Problem(s) to be Solved by the Invention] However, in cryptocommunication with the above encryption keys, this invention person found out that there were the following troubles.
[0005] That is, in order to hold the safety of cryptocommunication, it is a burden with periodically, remarkable although it is desirable to change by the manager of a communication device in a short cycle as it has stroked so that it may be called every several hours changing a cryptographic key every several hours about a cryptographic key, and is substantially difficult.
[0006] Moreover, according to the place which this invention person examined, there is also a problem which is explained below at the time of modification of a cryptographic key.
[0007] First, the cryptocommunication technique in network configuration is explained.
[0008] As shown in drawing 17 , the communication devices 30-32 which perform cryptocommunication, such as a personal computer, are connected to the network 40, respectively.
[0009] Here, the case where cryptocommunication is independently carried out, respectively between a communication device 30, a communication device 31 and a communication device 30, and a communication device 32 is explained.
[0010] The manager of each communication device sets the encryption key for carrying out other communication devices and cryptocommunication as the communication device which he manages, before starting other communication devices and a communication link. namely, the manager of a communication device 30 -- a communication device 31 and a communication device 32 -- respectively -- ** -- the cryptographic key Kab1 for cryptocommunication, and Kac1 It is set as a communication device 30, respectively. The manager of a communication device 31 is the cryptographic key Kab1 for carrying out cryptocommunication to a communication device 30. It is set as a communication device 31. The manager of a communication device 32 is the cryptographic key Kac1 for carrying out cryptocommunication to a communication device 30. It is set as a communication device 32.
[0011] Moreover, with a communication device 30, the packet addressed to communication device 31 is a

cryptographic key Kab1. It enciphers, and transmits to a communication device 31, and the packet addressed to communication device 32 is a cryptographic key Kac1. It enciphers and transmits to a communication device 32.
[0012] Furthermore, the packet which received from the communication device 31 in the communication device 30 is a cryptographic key Kab1. The packet which decrypted and received from the communication device 32 is a cryptographic key Kac1. It decrypts. The packet addressed to communication device 30 is a cryptographic key Kab1 similarly with a communication device 31. It enciphers, and transmits to a communication device 30, and the packet which received from the communication device 30 is decrypted by the cryptographic key Kab1. Also with a communication device 32, the packet addressed to communication device 30 is a cryptographic key Kac1. The packet which enciphered, transmitted to the communication device 30 and received from the communication device 30 is a cryptographic key Kac1. It decrypts.
[0013] Cryptocommunication is performed as mentioned above between a communication device 30 and a communication device 31 and between a communication device 30 and a communication device 32.
[0014] Next, drawing 16 explains the procedure when changing a cryptographic key, and drawing 17 explains a sequence.
[0015] First, in drawing 18 , axes of ordinate J1 and J2 are time-axes, and processing of a communication device 30 is shown in the left-hand side of a shaft J1, they show processing of a communication device 31 to the right-hand side of a shaft J2, respectively, and the commo data between a communication device 30 and a communication device 31 is expressed between the shaft J1 and the shaft J2.
[0016] Cryptographic key Kab1 used for cryptocommunication in a communication device 30 It sets up. Cryptographic key Kab1 similarly used for cryptocommunication with a communication device 31 It sets up. K (I) decides to express the data which enciphered Data I by the cryptographic key K here.
[0017] With a communication device 30, it is the data Ia addressed to communication device 31. Cryptographic key Kab1 It enciphers, the code data Kab (Ia) are generated, and it transmits to a communication device 31. The communication device 31 which received this is a cryptographic key Kab1 about the code data Kab (Ia). It decrypts and is Data Ia. It takes out.
[0018] Next, the case where a cryptographic key is changed is explained.
[0019] Since there is no means to change a cryptographic key into coincidence with a communication device 30 and a communication device 31, each modification will shift for a while in time. Here, it is assumed that modification of the cryptographic key in a communication device 30 arose previously.
[0020] a communication device 30 -- a cryptographic key -- Kab1 from -- it changes into K'ab1. Data Ib addressed to communication device 31 It enciphers by encryption key K'ab1, code data K'ab (Ib) is generated, and it transmits to a communication device 31. The communication device 31 which received K'ab (Ib) is the encryption key Kab1 about code data K'ab (Ib). It decrypts.
[0021] In this case, a communication device 31 is the original data Ib. It cannot take out. That is, it is K about what decrypted Data I by the cryptographic key K. If it is expressing (I), the value which the communication device 31 took out will serve as K ab !=(K'ab (Ib)) Ib.
[0022] Therefore, in order to solve the problem of the time lag of cryptographic key modification which occurs between the communication devices 30 and communication devices 31 which perform this cryptocommunication, cryptocommunication is interrupted temporarily, after changing the key of each communication device, cryptocommunication must be made to resume, and there is a problem that the communication link between communication devices must once be interrupted.
[0023] The purpose of this invention is to offer the storage which recorded the renewal approach of a cryptographic key and the renewal program of a cryptographic key which can change a cryptographic key, without making the load accompanying cryptographic key modification of a device-management person mitigate, and interrupting a communication link.
[0024]
[Means for Solving the Problem] The renewal approach of a cryptographic key of this invention creates the cryptographic key table which consisted of identifiers which specify two or more cryptographic key and each cryptographic key in the communication device which performs cryptocommunication. The 1st communication device of the communication devices which perform cryptocommunication chooses the identifier from a cryptographic key table. The 2nd communication device with which the identifier was notified to the 2nd communication device of the communication devices which perform

cryptocommunication, and the 1st communication device and identifier were notified takes out the cryptographic key corresponding to an identifier from this cryptographic key table.
[0025] Moreover, respectively the same master key is held, the 1st communication device of the communication devices which perform cryptocommunication generates a hash key, the communication device with which the renewal approach of a cryptographic key of this invention performs cryptocommunication notifies the hash key concerned to the 2nd communication device of the communication devices which perform cryptocommunication, and this 1st communication device and the 2nd communication device make it the cryptographic key which updated the result of having hashed the master key with the hash key.
[0026] Furthermore, the renewal approach of a cryptographic key of this invention creates the cryptographic key master table which consisted of identifiers which specify two or more cryptographic key and each cryptographic key in the communication device which performs cryptocommunication. The 1st communication device of the communication devices which perform cryptocommunication chooses one identifier from a cryptographic key master table. The identifier is notified to the 2nd communication device of the communication devices which perform cryptocommunication. The 1st communication device which performs cryptocommunication generates a hash key, and notifies the generated hash key to the 2nd communication device. The cryptographic key corresponding to the identifier as which the 1st communication device and 2nd communication device were chosen is taken out from a cryptographic key master table, and it considers as the cryptographic key which updated the result of having hashed the cryptographic key with the hash key.
[0027] Moreover, the step which creates the cryptographic key table which records correspondence with an identifier for the storage of this invention to specify two or more cryptographic key and each cryptographic key in the communication device which performs cryptocommunication, The step which chooses the identifier corresponding to one cryptographic key in two or more cryptographic keys, and this cryptographic key from a code table in case the communication device which performs cryptocommunication transmits data, It consists of a step which notifies the selected identifier to the communication device of a data transmission place, and a step which takes out the cryptographic key to which this identifier corresponds from a cryptographic key table according to reception of the identifier notified by cryptocommunication from other communication devices.
[0028] By the above thing, since it is necessary to make a change of a cryptographic key to no communication devices, a manager's burden can be mitigated sharply and the setting mistake of a cryptographic key can also be prevented.
[0029] Moreover, since it is not necessary to stop temporarily the communication device at the time of renewal of a cryptographic key, working efficiency can be improved.
[0030] Furthermore, since the updating data used in order to update a cryptographic key between communication devices are not cryptographic key itself, security can be raised sharply.
[0031] Moreover, it will be as follows if the outline of other solution means is explained briefly.
[0032] Other solution means are the updating approaches of a cryptographic key used in case two or more communication devices are connected in a network and cryptocommunication is performed among said two or more communication devices. The cryptographic key table which consisted of identifiers which specify two or more cryptographic key and each cryptographic key in the communication device which performs said cryptocommunication is created. The 1st communication device of said communication devices which perform cryptocommunication chooses an identifier from said cryptographic key table. It passes and notifies to the 2nd communication device of the communication devices which encipher the identifier by the cryptographic key and perform said cryptocommunication. Said 2nd notified communication device decodes the identifier enciphered by the cryptographic key. Said 2nd communication device which decoded said the 1st communication device and identifier takes out the cryptographic key corresponding to an identifier from said cryptographic key table, and cryptocommunication is performed between the said 1st and 2nd communication device using this cryptographic key.
[0033] Moreover, as for other solution means, two or more communication devices are connected in a network. It is the updating approach of a cryptographic key used in case cryptocommunication is performed among said two or more communication devices. The communication device which performs said cryptocommunication holds the same master key, respectively, and the 1st communication device generates a hash key among said communication devices which perform cryptocommunication. Encipher

said hash key by ****** and said enciphered hash key is notified to the 2nd communication device of the communication devices which perform said cryptocommunication. The hash key with which said 2nd communication device with which said hash key was notified was this enciphered by the cryptographic key is decoded, and cryptocommunication is performed between the said 1st and 2nd communication device by making into a cryptographic key the result to which said 1st and 2nd communication device hashed the master key with the hash key.

[0034] Furthermore, as for other solution means, two or more communication devices are connected in a network. It is the updating approach of a cryptographic key used in case cryptocommunication is performed among said two or more communication devices. The cryptographic key master table which consisted of identifiers which specify two or more cryptographic key and each cryptographic key in the communication device which performs said cryptocommunication is created. The 1st communication device of the communication devices which perform said cryptocommunication chooses the identifier of arbitration from said cryptographic key master table. It notifies to the 2nd communication device of the communication devices which encipher the identifier by the cryptographic key and perform said cryptocommunication. Said 1st communication device generates a hash key, enciphers said hash key by this cryptographic key, and notifies to said 2nd communication device. Said 2nd communication device with which the enciphered identifier was notified decodes the enciphered identifier and said hash key. The cryptographic key corresponding to an identifier is taken out from said cryptographic key master table, the result of having hashed the cryptographic key with said hash key is made into a cryptographic key, and cryptocommunication is performed between the said 1st and 2nd communication device using the cryptographic key.

[0035]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail based on a drawing.

[0036] (Gestalt 1 of operation) The block diagram of the cryptographic key table according [the explanatory view of cryptographic key modification processing according / the block diagram in the communication device according / the explanatory view of the network configuration in the communication device according / drawing 1 / to the gestalt 1 of operation of this invention and drawing 2 / to the gestalt 1 of operation of this invention, drawing 3 , and drawing 4 / to the gestalt 1 of operation of this invention and drawing 5] to the gestalt 1 of operation of this invention, drawing 6 , and drawing 7 are the flow charts of cryptographic key modification by the gestalt 1 of operation of this invention.

[0037] In the gestalt of this operation, the communication devices 1-3 with which the network configuration which performs cryptocommunication performs cryptocommunication, such as a personal computer, as shown in drawing 1 are connected to the network 4, respectively. Moreover, cryptocommunication shall be independently performed in this case, respectively between a communication device 1 and a communication device 2 and between a communication device 1 and a communication device 3.

[0038] Next, the configuration in a communication device 1 is explained using drawing 2 .

[0039] First, a communication device 1 is constituted by the bus controller 11 which performs control of CPU10 and the bus which manage all control of a floppy disk drive 5, a hard disk drive 6, CD-ROM drive 7, 81-8n of communication link controllers, main memory 9, and a communication device 1, and these are connected by the internal bus 12.

[0040] And a communications program and the cryptographic key table mentioned later are installed on a hard disk from a floppy disk drive 5 or CD-ROM drive 7, or performs loading to the direct main memory 9. Moreover, when it installs on a hard disk, loading shall be performed from a hard disk to main memory 9. Furthermore, it is also installable in other communication devices through a network 4 from a floppy disk drive 5 or CD-ROM drive 7.

[0041] In addition, a cryptographic key table may be stored in a floppy disk drive 5 or CD-ROM drive 7 in the form of a cryptographic key table, and may be generated by the cryptographic key table generator from other data.

[0042] 81-8n of next, communication link controllers The data transfer with transceiver buffer 9a which should perform only physical-level (below MAC layer) control, and was prepared in main memory 9 is 81-8n of communication link controllers. The prepared Direct Memory Access (DMA) performs. 81-8n of moreover, communication link controllers Forming CPU10 inside and operating a communications program

there and 81-8n of communication link controllers CPU10 is able to form a transceiver secondary buffer inside and to carry out data transfer between transceiver buffer 9a on main memory 9. Moreover, in drawing 2 , although the circuitry in a communication device 1 was explained, the other communication devices 2 and 3 are also considered as the same configuration.
[0043] Next, a setup of the cryptographic key in each communication device is explained.
[0044] First, as shown in drawing 3 , the cryptographic key table which performs cryptocommunication to each communication device 1-3, which has registered two or more cryptographic keys for every partner and which is mentioned later is set up. That is, the cryptographic key tables Tab and Tac used in order to carry out cryptocommunication to each of a communication device 2 and a communication device 3 are set to a communication device 1.
[0045] Moreover, the cryptographic key table Tab for performing a communication device 1 and cryptocommunication is set to a communication device 2, and the cryptographic key table Tac for performing a communication device 1 and cryptocommunication is set to a communication device 3.
[0046] Here, the cryptographic key table Tab of a communication device 1, the cryptographic key table Tab of a communication device 2, and the communication device 1 cryptographic-key table Tac and the cryptographic key table Tac of a communication device 3 are the same respectively. Furthermore, these consist of ID which is the identifiers of the arbitration corresponding to two or more cryptographic key and each key.
[0047] And it specifies [which key is used out of a cryptographic key table using this ID, and]. For example, in using the key of ID=5 by the cryptocommunication between a communication device 1 and a communication device 2, it sets ID=5 as each communication device 1 and 2 as initial value. Similarly, in using the key of ID=3 by the cryptocommunication between a communication device 1 and a communication device 3, it sets ID=3 as each communication device 1 and 3 as initial value.
[0048] Next, in each communication device 1-3, based on set-up ID, one cryptographic key is taken out from each cryptographic key table, it uses for the code of the data to transmit, and the decode of data which received, and cryptocommunication is performed.
[0049] For example, if the cryptographic key of ID=n is expressed as K [ID=n], the cryptographic key used, respectively by the cryptocommunication between a communication device 1 and a communication device 2 and between a communication device 1 and a communication device 2 will turn into a cryptographic key Kab [ID=5] and a cryptographic key Kac [ID=3], respectively.
[0050] Here, the case where the cryptographic key of the cryptocommunication between a communication device 1 and a communication device 2 is changed is explained using drawing 4 .
[0051] First, ID of a cryptographic key is changed into ID=8 with a communication device 1. In a communication device 1, the cryptographic key Kab equivalent to ID=8 [ID=8] is taken out from the cryptographic key table Tab.
[0052] ID=8 are transmitted to a communication device 2 as ID change command HC from a communication device 1 at this and coincidence. In a communication device 2, ID=8 are taken out from this ID change command HC, and the cryptographic key Kab equivalent to ID=8 [ID=8] is taken out from the cryptographic key table Tab.
[0053] By this, since the encryption key of a communication device 1 and a communication device 2 can be changed, the cryptocommunication between a communication device 1 and a communication device 2 becomes possible [continuing using the changed cryptographic key Kab [ID=8]].
[0054] In addition, as for a cryptographic key table, enciphering and holding is desirable. Moreover, as for ID change command HC, enciphering and transmitting is desirable. Furthermore, as for the cryptographic key when enciphering ID change command HC, it is desirable that it is an encryption key before modification. Moreover, Tac of the cryptographic key table Tab of a communication device 1 and a communication device 2, a communication device 1, and a communication device 3 may be the same.
[0055] That is, or it is plurality, the same cryptographic key table may be used in the cryptocommunication between all the communication devices 1-3. In that case, the number of the same cryptographic key tables set to a communication device 1 may be one, and ID may also use the same ID among two or more communication devices.
[0056] Moreover, the manager of a communication device may specify ID to change and it may be chosen with the random number in a communication device 1-3.
[0057] Next, the configuration of the cryptographic key table Tab (drawing 3) is shown in drawing 5 .

[0058] The cryptographic key table Tab consists of a field holding two or more cryptographic keys Kab, and a field holding ID which is an identifier corresponding to it.
[0059] The procedure in a communication device 1 is explained using the processing flow shown in drawing 3 - drawing 5 , and drawing 6 .
[0060] First, cryptographic key Kz by which CPU10 performs a setup of ID=5 with the cryptographic key table Tab (step S101), and is equivalent to ID=5 from the cryptographic key table Tab with initial setting It chooses (step S102).
[0061] Next, CPU10 sets a transmitting counter as zero (step S103), and starts cryptocommunication (step S104). And CPU10 is a cryptographic key Kz about the packet addressed to communication device 2. It enciphers, and transmits to a network 4 (step S105), and a transmitting counter is incremented one time (step S106).
[0062] Then, when a transmitting counter is less than 100, the cryptocommunication addressed to return and communication device 2 is repeated to processing of step S105.
[0063] Moreover, CPU10 shifts to an update process of ID, when a transmitting counter is 100 or more (step S107). CPU10 chooses ID=8 [new] with a random number (step S108), and is a cryptographic key Kx about the ID=8. The enciphered data Kx [ID=8] are added to ID change command HC, and it transmits to a communication device 2 to a network 4 (step S109).
[0064] And cryptographic key Ku corresponding to ID=8 from return and the cryptographic key table Tab to processing of step S102 It takes out. Then, it is a cryptographic key Ku until it resets a transmitting counter to zero and a transmitting counter becomes 100 or more henceforth. It transmits by using and enciphering the packet addressed to communication device 2.
[0065] Next, the procedure in a communication device 2 is explained using drawing 3 - drawing 5 , and drawing 7 .
[0066] First, cryptographic key Kz which is equivalent to ID=5 from the cryptographic key table Tab after CPU10 sets up the cryptographic key table Tab and ID=5 by initial setting (step 201) It chooses (step S202).
[0067] Next, the packet which received from the communication device 1 is written in transceiver buffer 9a, and CPU10 is a cryptographic key Kz. It uses and decodes (step S203). The packet which decoded CPU10 distinguishes whether it is ID change command HC (step S204).
[0068] And when this packet is not ID change command HC, CPU10 performs reception (for example, data are handed over to application) which was adapted for this packet (step S205), and returns to processing of step S203. On the other hand, when this packet is the ID change command 33, CPU10 takes out ID=8 changed from this packet (step S206).
[0069] And cryptographic key Ku corresponding to ID=8 of return and the cryptographic key table Tab to processing of step S202 It takes out. henceforth -- until it receives new ID change command -- until cryptographic key Ku The packet which used and received from the communication device 1 is decrypted.
[0070] Between a communication device 1 and a communication device 2, it is a cryptographic key Kz until ID change command HC is sent from a communication device 1 as mentioned above. After it used and ID change command HC was received by the communication device 2, between a communication device 1 and a communication device 2, it is a cryptographic key Ku. It can use and cryptocommunication can be performed.
[0071] Therefore, a communication device manager only sets the cryptographic key table Tab and ID=5 as a communication device 1 and a communication device 2 as initialization information, respectively, and, after that, a key is updated automatically.
[0072] Moreover, with the gestalt of this operation, although the decision value of a transmitting counter was set as 100, a manager may set up this decision value freely. Moreover, as for the cryptographic key table Tab, holding to the field which cannot access except a manager is desirable, and it is desirable to encipher and hold the cryptographic key table Tab itself by another cryptographic key.
[0073] Here, in order to usually decode a cipher, huge time amount and computer power are needed. However, it cannot declare that it is impossible to find out a cryptographic key also by chance. Therefore, if the cryptographic key is used at all when a third person gets a cryptographic key by chance, all ciphers will become decipherable for a third person.
[0074] Then, in the gestalt 1 of this operation, it is made to make the evil by the above-mentioned trouble by changing a cryptographic key periodically into the minimum.

[0075] That is, if a third person gets a cryptographic key also by chance as mentioned above, a third person will become possible [decoding a cipher using the cryptographic key]. Since the cryptographic key is changed periodically, it becomes impossible however, for a third person to decode a cipher.
[0076] Thus, very primary that a cipher is decoded and all data are not decoded. Furthermore, the data decoded can be pressed down by shortening modification spacing of a cryptographic key to the minimum.
[0077] (Gestalt 2 of operation) The explanatory view of cryptographic key modification processing according [drawing 8 and drawing 9] to the gestalt 2 of operation of this invention, drawing 10 , and drawing 11 are the flow charts of cryptographic key modification by the gestalt 2 of operation of this invention.
[0078] In the gestalt 2 of this operation, drawing 1 mentioned above and the procedure of setting a cryptographic key as each communication device 1-3 in the same system configuration as drawing 2 are explained using drawing 8 .
[0079] First, the hash key HK for generating a cryptographic key, applying a hash to the master key MK and the master key MK for every partner who performs cryptocommunication to each communication device 1-3 is set up.
[0080] That is, the master keys MKab and MKac for generating the cryptographic key used when performing cryptocommunication with a communication device 2 and a communication device 3, respectively, and the hash keys HKab and HKac are set to a communication device 1.
[0081] Moreover, the master key MKab for generating the cryptographic key used when using a communication device 1 and cryptocommunication, and the hash key HKab are set to a communication device 2. In addition, the master key MKab of a communication device 1, the master key MKab of a communication device 2, and the hash key HKab of a communication device 1 and the hash key HKab of a communication device 2 are the same respectively.
[0082] The master key MKac for generating the cryptographic key which similarly is used for it when performing a communication device 1 and cryptocommunication also to a communication device 3, and the hash key HKac are set up. In addition, the master key MKac of a communication device 1, the master key MKac of a communication device 3, and the hash key HKac of a communication device 1 and the hash key HKac of a communication device 3 are the same respectively.
[0083] In each communication device 1-3, encryption key K=HK (MK) is generated from the master key MK and the hash key HK. In order to perform cryptocommunication between a communication device 1 and a communication device 2, in a communication device 1 and a communication device 2, a cryptographic key HKab (MKab) is generated, respectively. Moreover, between a communication device 1 and a communication device 2, cryptocommunication is performed using this cryptographic key HKKab (MKab).
[0084] Here, the procedure of changing a cryptographic key is explained using drawing 9 .
[0085] First, a hash key is changed in a communication device 1. The manager of a communication device 1 may perform the modification approach, and it may be searched for from the random number in a communication device.
[0086] If the hash key of a communication device 1 is changed into hash key HK'ab, encryption key K=HK'ab (MKab) will be generated in a communication device 1. A communication device 1 transmits changed hash key HK'ab to a communication device 2 with the hash key change command HHC at coincidence. The communication device 2 which received the hash key change command HHC takes out hash key HK'ab from this hash key change command HHC, and generates cryptographic key HK'ab (MKab) using this hash key HK'ab.
[0087] Henceforth, cryptocommunication is performed using cryptographic key HK'ab (MKab) between a communication device 1 and a communication device 2. In addition, a master key and a hash key are enciphered and held, and are as desirable as Lycium chinense, and it is desirable to also encipher and transmit the hash key change command HHC.
[0088] Moreover, as for the encryption key when enciphering the hash key change command HHC, it is desirable to use the cryptographic key before modification. Furthermore, even when both a master key, a hash key or a master key, and a hash key are the same at plurality or all communication devices, it is good. In that case, you may use it in common [without holding the same master key or the same hash key for every communications partner within one communication device].
[0089] Next, the procedure in a communication device 1 is explained using the processing flow shown in drawing 8 , drawing 9 , and drawing 10 .

[0090] First, by initial setting, CPU10 sets up the master key MKab and the hash key HKab (step S301), and sets a transmitting timer to zero (step S302). In addition, this transmitting timer shall be automatically updated in another task, or renewal of automatic shall be carried out by hardware.
[0091] And CPU10 sets the result (=HKab (MKab)) of having hashed the master key with the hash key as a cryptographic key K (step S303), and starts cryptocommunication (step S304).
[0092] The packet addressed to communication device 2 is enciphered by the cryptographic key K, and it transmits to a network 4 (step S305). Then, a transmitting timer is read (step S306) and it judges whether the transmitting timer is over 5 minutes (step S307).
[0093] Here, when this transmitting timer is less than 5 minutes, the following packet addressed to return and communication device 2 is enciphered to processing of step S304 by the cryptographic key K, and it transmits to it to a network 4.
[0094] On the other hand, when this transmitting timer is over 5 minutes, an internal random number generates new hash key HK'ab (step S308), new hash key HK'ab is enciphered by the cryptographic key K, the this enciphered data are added to the hash key change command 47, and it transmits to the addressing network 4 to communication device 2 (step S309), it returns to step S302, and a transmitting timer is again set to zero.
[0095] Then, the result (= HK'ab (MKab)) of having hashed the master key MKab by new hash key HK'ab is set as the new cryptographic key K. Henceforth, the packet addressed to communication device 2 is enciphered using the new cryptographic key K until a transmitting timer value exceeds 5 minutes, and the this enciphered packet is transmitted to a network 4.
[0096] Next, the procedure in a communication device 2 is explained using drawing 8 , drawing 9 , and drawing 11 .
[0097] First, CPU10 sets up the master key MKab and the hash key HKab by initial setting (step S401). And the result (=HKab (MKab)) to which CPU10 hashed the master key with the hash key is set as a cryptographic key K (step S402).
[0098] If the packet transmitted from the communication device 1 is received from a network 4, this packet will be written in transceiver buffer 9a, and CPU10 will decrypt by the cryptographic key K (step S403). It judges whether the packet which CPU10 this decoded is the hash key change command HHC (step S404).
[0099] And when it is not the hash key change command HHC, CPU10 performs reception (for example, data are handed over to application) which was adapted for this packet (step S405), and returns to processing of step S403.
[0100] On the other hand, when this packet is the hash key change command HHC, CPU10 takes out hash key HK'ab changed from this packet (step S406). And the result (= HK'ab (MKab)) hashed by new hash key HK'ab which took [above-mentioned] out return and the master key MKab picking is set as processing of step S402 as a new cryptographic key K. Henceforth, the packet which received from the communication device 1 using the cryptographic key K is decrypted until it receives a new hash key change command.
[0101] After the hash key change command HHC is received by the communication device 2 using a cryptographic key K (=HKab (MKab)), between a communication device 1 and a communication device 2, cryptocommunication can be performed between a communication device 1 and a communication device 2 using a cryptographic key K (=HK'ab (MKab)), until the hash key change command HHC is sent from a communication device 1 as mentioned above.
[0102] Therefore, renewal of a key will be automatically performed only by a communication device manager setting the master key MKab and the hash key HKab as a communication device 1 and a communication device 2 as initialization information, respectively.
[0103] In addition, in the gestalt 2 of this operation, although the decision value of a transmitting timer was set up in 5 minutes, a manager may set up this decision value freely. Moreover, as for the master key MKab and the hash key HKab, holding to the field which cannot access except a manager is desirable. It is desirable to encipher and hold the master key MKab and the hash key HKab itself by another cryptographic key furthermore.
[0104] Moreover, it can prevent that make decode of a cipher very into a primary thing, and all data are decoded by changing a cryptographic key periodically also with the gestalt 2 of this operation. Furthermore, the data decoded can be pressed down by shortening modification spacing of a cryptographic key to the minimum.

[0105] (Gestalt 3 of operation) The cryptographic key master table according [the explanatory view of cryptographic key modification processing according / drawing 12 and drawing 13 / to the gestalt 3 of operation of this invention and drawing 14] to the gestalt 3 of operation of this invention, drawing 15 , and drawing 16 are the flow charts of cryptographic key modification by the gestalt 3 of operation of this invention.
[0106] The gestalt 3 of this operation explains drawing 1 mentioned above and the procedure of setting a cryptographic key as each communication device 1-3 in the same system configuration as drawing 2 , using drawing 12 .
[0107] The same cryptographic key master table MT is set to each communication device 1-3. This code master table key MT consists of ID corresponding to two or more cryptographic keys (MK [ID]) and it.
[0108] K=HK (MK [ID]) which hashed two or more cryptographic keys MK [ID] with the hash key HK generates the cryptographic key K when actually performing cryptocommunication. Here, if ID and the hash key for generating the cryptographic key for the cryptocommunication between a communication device 1 and a communication device 2 are set as a communication device 1 and a communication device 2 with ID=6 and HKab, respectively, in a communication device 1 and a communication device 2, cryptographic key K=HKab (MK [6]) will be generated, respectively.
[0109] And cryptocommunication is performed using this cryptographic key K. If ID and the hash key for generating the cryptographic key for the cryptocommunication between a communication device 1 and a communication device 3 similarly are set to ID=8 and HKac at a communication device 1 and a communication device 2, respectively, in a communication device 1 and a communication device 2, cryptographic key K=HKac (MK [8]) will be generated, respectively. And cryptocommunication is performed using this cryptographic key K.
[0110] Next, the procedure of changing the cryptographic key between a communication device 1 and a communication device 2 is explained using drawing 13 .
[0111] First, ID and the hash key of a communication device 1 are changed into ID=5 and hash key HK'ab, respectively. Cryptographic key K=HK'ab (MK [5]) is generated in a communication device 1.
[0112] It can come, simultaneously a communication device 1 notifies ID=5 and hash key HK'ab which were changed to a communication device 2 with the key change command KHC. The communication device 2 which received this key change command KHC takes out ID=5 and hash key HK'ab from this key change command KHC, and generates cryptographic key K=HK'ab (MK [5]). between a communication device 1 and a communication device 2 -- this -- ****** -- cryptocommunication is performed using a cryptographic key K.
[0113] In addition, as for a cryptographic key master table, enciphering and holding is desirable. As for a key change command, enciphering and transmitting is desirable. As for the cryptographic key when enciphering a key change command, it is desirable that it is the cryptographic key before changing. Although [a cryptographic key master table / with a system] it is the same, another table may be used for it for every communications partner. Although it was made the value of the proper for every communications partner, even if ID and a hash key are common to a system in ID, a hash key, or both, they are good.
[0114] Next, the configuration of the cryptographic key master table MT is shown in drawing 14 .
[0115] The cryptographic key master table MT consists of a field holding two or more cryptographic keys K, and a field holding the identifier ID corresponding to it.
[0116] Here, the procedure in a communication device 1 is explained using the processing flow shown in drawing 12 - drawing 14 , and drawing 15 .
[0117] First, CPU10 sets up the cryptographic key master table MT, and ID=6 and the hash key HKab by initial setting (step S501). Next, CPU10 is the code master key Kw which is equivalent to ID=6 from the cryptographic key master table MT. It chooses and is this master cryptographic key Kw. The result (=HKab (Kw)) hashed with the hash key HKab is set up as a cryptographic key K (step S502), and cryptocommunication is started (step S503).
[0118] And it judges whether the packet addressed to communication device 2 is enciphered by the cryptographic key K, it transmits to a network 4 (drawing 1) (step S504), and CPU10 has a cryptographic key change request (step S505).
[0119] Here, this cryptographic key change request is using a manager interface and directing modification (it being specifically a setup of new ID and a hash key) of a cryptographic key, in order that a manager's

may change a cryptographic key, and the key change-request flag which the program of a communication device can read is set by these directions. Moreover, it is judged that the program of a communication device has a cryptographic key change request by having set this key change-request flag.
[0120] Next, when the manager is not performing the change request of a cryptographic key, since this cryptographic key change-request flag is not set, return and the packet addressed to communication device 2 are again enciphered by the cryptographic key K succeedingly to processing of step S504, and this packet is transmitted to a network 4.
[0121] On the other hand, when a manager performs the change request of a cryptographic key with a predetermined input means, by CPU10, ID=5 and hash key HK'ab which the cryptographic key change-request flag was set up on main memory 9, and were set up newly are read, and this cryptographic key change-request flag is reset (step S506).
[0122] CPU10 is this reading **** -- the data which enciphered ID=5 and hash key HK'ab by the cryptographic key K are added to the key change command KHC, and it transmits to a communication device 2 to a network 4 (step S507).
[0123] Cryptographic key Ky corresponding to ID=5 from return and the cryptographic key master table MT to processing of step S502 It takes out. And it is a cryptographic key Ky until a cryptographic key change-request flag is set. It uses, and the packet addressed to communication device 2 is enciphered, and it transmits.
[0124] Next, the procedure in a communication device 2 is explained using drawing 12 - drawing 14 , and drawing 17 .
[0125] First, CPU10 sets up the cryptographic key master table MT, and ID=6 and the hash key HKab by initial setting (step S601). CPU10 is the code master key Kw which is equivalent to ID=6 from the cryptographic key master table MT. It chooses and is this master cryptographic key Kw. The result (=HKab (Kw)) hashed with the hash key HKab is set up as a cryptographic key K (step S602).
[0126] And CPU10 is a cryptographic key Kw about the packet which received from the communication device 1. It decodes by using (step S603). The decoded this packet performs reception (for example, data are handed over to application) by which CPU10 was adapted for this packet when this packet was not the key change command KHC by CPU10 distinguishing whether it is the key change command KHC (step S604) (step S605), and it returns to processing of step S603.
[0127] On the other hand, when this packet is the key change command KHC, CPU10 takes out ID=5 and hash key HK'ab which were changed from this packet (step S606).
[0128] And cryptographic key Ky corresponding to ID=5 of return and the cryptographic key master table MT to step S602 It takes out. Henceforth, it is a cryptographic key Ky until it receives a new key change command. The packet which used and received from the communication device 1 is decrypted.
[0129] Between a communication device 1 and a communication device 2, it is a cryptographic key Kw until the key change command KHC is sent from a communication device 1 as mentioned above. After it used and the key change command KHC was received by the communication device 2, between a communication device 1 and a communication device 2, it is a cryptographic key Ky. It can use and cryptocommunication can be performed.
[0130] Therefore, a communication device manager sets the cryptographic key master table MT and ID=6 as a communication device 1 and a communication device 2 as initialization information, respectively, required information will only be set as one communication device to change a key, and, after that, renewal of a key will be performed automatically.
[0131] In addition, as for the cryptographic key master tables MT and ID and a hash key, holding to the field which cannot access except a manager is desirable. Furthermore, as for the cryptographic key master tables MT and ID and a hash key, it is desirable to encipher and hold itself by another cryptographic key.
[0132] Moreover, it can prevent that make decode of a cipher very into a primary thing, and all data are decoded by changing a cryptographic key periodically also according to the gestalt 3 of this operation. Furthermore, the data decoded can be pressed down by shortening modification spacing of a cryptographic key to the minimum.
[0133] It cannot be overemphasized that it can change variously in the range which this invention is not limited to the gestalt of said operation, and does not deviate from the summary.
[0134] For example, with the gestalten 1-3 of said operation, in between mutual communication devices, although the updating technique of a cryptographic key using the table according to individual was

indicated, two or more three or more communication devices may be made to update the common **** cryptographic key for tables.
[0135] Moreover, in the gestalten 1-3 of said operation, a data encryption and enciphered processing of the double sign of data may be realized by any of software or hardware.
[0136]
[Effect of the Invention]
(1) According to this invention, since it is necessary to make a change of a cryptographic key to no communication devices, a manager's burden can be mitigated sharply and the setting mistake of a cryptographic key can also be prevented.
[0137] (2) Moreover, in this invention, since the data which set and are carried out between communication devices at the time of renewal of a cryptographic key are not cryptographic key itself, security can be raised sharply.
[0138] (3) Since it is not necessary to set to this invention and to stop temporarily the communication device at the time of renewal of a cryptographic key further, working efficiency can be improved more.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the explanatory view of the network configuration in the communication device by the gestalt 1 of operation of this invention.
[Drawing 2] It is a block diagram in the communication device by the gestalt 1 of operation of this invention.
[Drawing 3] It is the explanatory view of the cryptographic key modification processing by the gestalt 1 of operation of this invention.
[Drawing 4] It is the explanatory view of the cryptographic key modification processing by the gestalt 1 of operation of this invention.
[Drawing 5] It is the block diagram of the cryptographic key table by the gestalt 1 of operation of this invention.
[Drawing 6] It is the flow chart of cryptographic key modification by the gestalt 1 of operation of this invention.
[Drawing 7] It is the flow chart of cryptographic key modification by the gestalt 1 of operation of this invention.
[Drawing 8] It is the explanatory view of the cryptographic key modification processing by the gestalt 2 of operation of this invention.
[Drawing 9] It is the explanatory view of the cryptographic key modification processing by the gestalt 2 of operation of this invention.
[Drawing 10] It is the flow chart of cryptographic key modification by the gestalt 2 of operation of this invention.
[Drawing 11] It is the flow chart of cryptographic key modification by the gestalt 2 of operation of this invention.
[Drawing 12] It is the explanatory view of the cryptographic key modification processing by the gestalt 3 of operation of this invention.
[Drawing 13] It is the explanatory view of the cryptographic key modification processing by the gestalt 3 of operation of this invention.
[Drawing 14] It is a cryptographic key master table by the gestalt 3 of operation of this invention.
[Drawing 15] It is the flow chart of cryptographic key modification by the gestalt 3 of operation of this invention.
[Drawing 16] It is the flow chart of cryptographic key modification by the gestalt 3 of operation of this invention.
[Drawing 17] It is the explanatory view of the cryptographic key modification processing which this invention person considered.
[Drawing 18] It is a sequence diagram in the cryptographic key modification processing which this invention person considered.
[Description of Notations]
1-3 [-- A hard disk drive, 7 / -- A CD-ROM drive and 81-8n / -- / -- A transceiver buffer, 10 / -- CPU, 11 / -- Bus controller, / A communication link controller, 9 -- Main memory 9a] -- A communication device, 4 -- A network, 5 -- A floppy disk drive, 6 12 [-- Master key --, HK / -- A hash key, HHC / -- A hash key change command, MT / -- A cryptographic key master table, KHC / -- Key

change command.] -- An internal bus, Tab, Tac -- A cryptographic key table, Kab, Kac -- A cryptographic key, a HC--ID change command, MK

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－55242

(43)公開日　平成11年(1999)２月26日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ
			６０１Ｅ

審査請求　未請求　請求項の数４　ＯＬ　（全 14 頁）

(21)出願番号　特願平9－208198

(22)出願日　平成９年(1997)８月１日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　大浦　哲生
神奈川県海老名市下今泉810番地　株式会社日立製作所オフィスシステム事業部内
(72)発明者　新　善文
神奈川県海老名市下今泉810番地　株式会社日立製作所オフィスシステム事業部内
(74)代理人　弁理士　筒井　大和

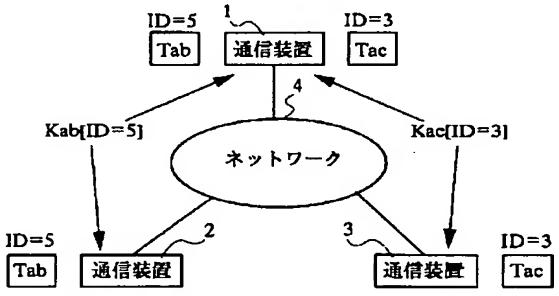
(54)【発明の名称】　暗号鍵更新方法および暗号鍵更新プログラムを記録した記憶媒体

(57)【要約】

【課題】　装置管理者の暗号鍵変更に伴う負荷を軽減させ、かつ通信を中断することなく暗号鍵の変更を行う。

【解決手段】　暗号通信を行う通信装置１～３に複数の暗号鍵Kab，Kacとそれぞれに付した識別子ＩＤをもつ暗号鍵テーブルを設け、その識別子を交換することにより暗号鍵Kab，Kacを更新する。

図　3



【特許請求の範囲】

【請求項１】　複数の通信装置がネットワークで接続され、前記複数の通信装置の間で暗号通信を行う際に用いる暗号鍵の更新方法であって、前記暗号通信を行う通信装置において複数の暗号鍵と各暗号鍵を特定する識別子から構成された暗号鍵テーブルを作成し、暗号通信を行う前記通信装置のうちの第１の通信装置が前記暗号鍵テーブルからの識別子を選択し、その識別子を前記暗号通信を行う通信装置のうちの第２の通信装置へ通知し、前記第１の通信装置および識別子が通知された前記第２の通信装置が識別子に対応する暗号鍵を前記暗号鍵テーブルから取り出すことを特徴とする暗号鍵更新方法。

【請求項２】　複数の通信装置がネットワークで接続され、前記複数の通信装置の間で暗号通信を行う際に用いる暗号鍵の更新方法であって、前記暗号通信を行う通信装置はそれぞれ同一のマスタ鍵を保持し、暗号通信を行う前記通信装置のうちの第１の通信装置がハッシュ鍵を生成し、前記ハッシュ鍵を前記暗号通信を行う通信装置のうちの第２の通信装置へ通知し、前記第１の通信装置ならびに前記第２の通信装置が、前記マスタ鍵を前記ハッシュ鍵によってハッシュした結果を更新した暗号鍵とすることを特徴とすることを暗号鍵更新方法。

【請求項３】　複数の通信装置がネットワークで接続され、前記複数の通信装置の間で暗号通信を行う際に用いる暗号鍵の更新方法であって、前記暗号通信を行う通信装置において複数の暗号鍵と各暗号鍵を特定する識別子から構成された暗号鍵マスタテーブルを作成し、前記暗号通信を行う通信装置のうちの第１の通信装置が前記暗号鍵マスタテーブルから一つの識別子を選択し、その識別子を前記暗号通信を行う通信装置のうちの第２の通信装置へ通知し、暗号通信を行う前記第１の通信装置がハッシュ鍵を生成し、生成したハッシュ鍵を前記第２の通信装置に通知し、前記第１の通信装置および前記第２の通信装置が前記選択された識別子に対応する暗号鍵を前記暗号鍵マスタテーブルから取り出し、前記暗号鍵を前記ハッシュ鍵によってハッシュした結果を更新した暗号鍵とすることを特徴とする暗号鍵更新方法。

【請求項４】　ネットワークで接続された複数の通信装置の間で暗号通信を行う際に用いる暗号鍵を更新するプログラムを記録する記憶媒体であって、前記プログラムは、暗号通信を行う通信装置において複数の暗号鍵と各暗号鍵を特定するための識別子との対応を記録する暗号鍵テーブルを作成するステップと、暗号通信を行う通信装置がデータを送信する際に前記暗号テーブルから前記複数の暗号鍵のうちの一つの暗号鍵と該暗号鍵に対応する識別子とを選択するステップと、前記選択した識別子をデータ送信先の通信装置に通知するステップと、暗号通信により他の通信装置から通知された前記識別子の受信に応じて、前記暗号鍵テーブルから該識別子の対応する暗号鍵を取り出すステップとからなることを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号鍵更新方法および暗号鍵更新プログラムを記録した記憶媒体に関し、特に、通信装置間での暗号通信時に用いられる暗号鍵の更新に適用して有効な技術に関するものである。

【０００２】

【従来の技術】本発明者が検討したところによれば、たとえば、パーソナルコンピュータなどの通信装置がネットワーク接続されたシステムにおいて、暗号通信が行われる通信装置間には、相互にやりとりをするデータの暗号化ならびに復号化の際に用いられる暗号化鍵が共有されており、その暗号鍵を用いることにより暗号通信が行われている。

【０００３】なお、この種のネットワークの暗号化通信技術について詳しく述べてある例としては、１９９６年７月３０日、株式会社オーム社発行、Ｄ．Ｂｒｅｎｔ Ｃｈａｐｍａｎ、Ｅｌｉｚａｂｅｔｈ Ｄ．Ｚｗｉｃｋｙ（著）、「ファイヤウォール構築　インターネット・セキュリテ」Ｐ３９３があり、この文献には、インターネットにおけるネットワークレベル暗号化の鍵の配布について記載されている。

【０００４】

【発明が解決しようとする課題】ところが、上記のような暗号化鍵による暗号通信では次のような問題点があることを本発明者は見い出した。

【０００５】すなわち、暗号通信の安全性を保持するために、暗号鍵を定期的かつ数時間毎というようなできるだけ短いサイクルで通信装置の管理者により変更していくことが望ましいが、暗号鍵の変更を数時間毎に行うことはかなりの負担であり、実質的には困難となっている。

【０００６】また、本発明者が検討したところによれば、暗号鍵の変更時には以下に説明するような問題もある。

【０００７】まず、ネットワーク構成における暗号通信技術について説明する。

【０００８】図１７に示すように、パーソナルコンピュータなどの暗号通信を行う通信装置３０～３２が、それぞれネットワーク４０に接続されている。

【０００９】ここで、通信装置３０と通信装置３１および通信装置３０と通信装置３２の間でそれぞれ独立に暗号通信をする場合について説明する。

【００１０】それぞれの通信装置の管理者は、他の通信装置と通信を開始する前に他の通信装置と暗号通信をするための暗号化鍵を自分が管理する通信装置に設定する。すなわち通信装置３０の管理者は、通信装置３１と通信装置３２それぞれとの暗号通信のための暗号鍵Kab_1，Kac_1をそれぞれ通信装置３０に設定する。通信装

置３１の管理者は、通信装置３０と暗号通信するための暗号鍵Kab_1を通信装置３１に設定する。通信装置３２の管理者は通信装置３０と暗号通信するための暗号鍵Kac_1を通信装置３２に設定する。

【００１１】また、通信装置３０では、通信装置３１宛のパケットは暗号鍵Kab_1で暗号化して通信装置３１宛に送信し、通信装置３２宛のパケットは暗号鍵Kac_1で暗号化して通信装置３２宛に送信する。

【００１２】さらに、通信装置３０では、通信装置３１から受信したパケットは暗号鍵Kab_1で復号化し、通信装置３２から受信したパケットは暗号鍵Kac_1で復号化する。通信装置３１でも同様に通信装置３０宛のパケットは暗号鍵Kab_1で暗号化して通信装置３０宛に送信し、通信装置３０から受信したパケットは暗号鍵Kab_1で復号化する。通信装置３２でも、通信装置３０宛のパケットは暗号鍵Kac_1で暗号化して通信装置３０に送信し、通信装置３０から受信したパケットは暗号鍵Kac_1で復号化する。

【００１３】以上のようにして通信装置３０と通信装置３１間および通信装置３０と通信装置３２間で暗号通信を行う。

【００１４】次に、暗号鍵を変更するときの手順を図１６により、シーケンスを図１７により説明する。

【００１５】まず、図１８において、縦軸Ｊ１，Ｊ２は時間軸であり、通信装置３０の処理を軸Ｊ１の左側に、通信装置３１の処理を軸Ｊ２の右側にそれぞれ示し、軸Ｊ１と軸Ｊ２の間は通信装置３０と通信装置３１の間の通信データを表している。

【００１６】通信装置３０では、暗号通信に使う暗号鍵Kab_1を設定する。同様に通信装置３１でも暗号通信に使う暗号鍵Kab_1を設定する。ここでK（I）は、データＩを暗号鍵Kで暗号化したデータを表すこととする。

【００１７】通信装置３０では、通信装置３１宛のデータＩａを暗号鍵Kab_1で暗号化し暗号データKab（Ｉａ）を生成し、通信装置３１宛に送信する。これを受信した通信装置３１は、暗号データKab（Ｉａ）を暗号鍵Kab_1で復号化しデータＩａを取り出す。

【００１８】次に、暗号鍵を変更する場合について説明する。

【００１９】通信装置３０と通信装置３１で同時に暗号鍵を変更する手段がないのでそれぞれの変更は時間的に少しずれることになる。ここで、通信装置３０での暗号鍵の変更が先に生じたと仮定する。

【００２０】通信装置３０では、暗号鍵をKab_1から$K'ab_1$に変更する。通信装置３１宛のデータＩｂを暗号化鍵$K'ab_1$で暗号化し、暗号データK'ab（Ｉｂ）を生成し、通信装置３１宛に送信する。K'ab（Ｉｂ）を受信した通信装置３１は、暗号データK'ab（Ｉｂ）を暗号化鍵Kab_1で復号化する。

【００２１】この場合、通信装置３１は、元のデータＩｂを取り出すことはできない。すなわち、暗号鍵Kでデータ Ｉを復号化したものをK（Ｉ）と表すこととすると、通信装置３１が取り出した値はK ab（K' ab（Ｉｂ））≠Ｉｂとなる。

【００２２】よって、この暗号通信を行う通信装置３０と通信装置３１との間で起きる暗号鍵変更の時間的ずれの問題を解決するためには、暗号通信を一時中断し、それぞれの通信装置の鍵を変更した後に暗号通信を再開させなければならず、通信装置間の通信を一旦中断しなければならないという問題がある。

【００２３】本発明の目的は、装置管理者の暗号鍵変更に伴う負荷を軽減させ、かつ通信を中断することなく暗号鍵の変更を行うことのできる暗号鍵更新方法および暗号鍵更新プログラムを記録した記憶媒体を提供することにある。

【００２４】

【課題を解決するための手段】本発明の暗号鍵更新方法は、暗号通信を行う通信装置において複数の暗号鍵と各暗号鍵を特定する識別子から構成された暗号鍵テーブルを作成し、暗号通信を行う通信装置のうちの第１の通信装置が暗号鍵テーブルからの識別子を選択し、その識別子を暗号通信を行う通信装置のうちの第２の通信装置へ通知し、第１の通信装置および識別子が通知された第２の通信装置が識別子に対応する暗号鍵を該暗号鍵テーブルから取り出すものである。

【００２５】また、本発明の暗号鍵更新方法は、暗号通信を行う通信装置はそれぞれ同一のマスタ鍵を保持し、暗号通信を行う通信装置のうちの第１の通信装置がハッシュ鍵を生成し、当該ハッシュ鍵を暗号通信を行う通信装置のうちの第２の通信装置へ通知し、該第１の通信装置ならびに第２の通信装置が、マスタ鍵をハッシュ鍵によってハッシュした結果を更新した暗号鍵とするものである。

【００２６】さらに、本発明の暗号鍵更新方法は、暗号通信を行う通信装置において複数の暗号鍵と各暗号鍵を特定する識別子から構成された暗号鍵マスタテーブルを作成し、暗号通信を行う通信装置のうちの第１の通信装置が暗号鍵マスタテーブルから一つの識別子を選択し、その識別子を暗号通信を行う通信装置のうちの第２の通信装置へ通知し、暗号通信を行う第１の通信装置がハッシュ鍵を生成し、生成したハッシュ鍵を第２の通信装置に通知し、第１の通信装置および第２の通信装置が選択された識別子に対応する暗号鍵を暗号鍵マスタテーブルから取り出し、暗号鍵をハッシュ鍵によってハッシュした結果を更新した暗号鍵とするものである。

【００２７】また、本発明の記憶媒体は、暗号通信を行う通信装置において複数の暗号鍵と各暗号鍵を特定するための識別子との対応を記録する暗号鍵テーブルを作成するステップと、暗号通信を行う通信装置がデータを送信する際に暗号テーブルから複数の暗号鍵のうちの一つ

の暗号鍵と該暗号鍵に対応する識別子とを選択するステップと、選択した識別子をデータ送信先の通信装置に通知するステップと、暗号通信により他の通信装置から通知された識別子の受信に応じて、暗号鍵テーブルから該識別子の対応する暗号鍵を取り出すステップとからなるものである。

【００２８】以上のことにより、暗号鍵の変更をすべての通信装置に対して行わなくてよいので、管理者の負担を大幅に軽減でき、かつ暗号鍵の設定ミスも防止することができる。

【００２９】また、暗号鍵の更新時における通信装置を一時的に停止させなくてよいので、作業効率を向上することができる。

【００３０】さらに、通信装置間において、暗号鍵を更新するために用いられる更新データが暗号鍵それ自体ではないので、セキュリティを大幅に向上させることができる。

【００３１】また、その他の解決手段の概要を簡単に説明すれば以下のとおりである。

【００３２】その他の解決手段は、複数の通信装置がネットワークで接続され、前記複数の通信装置の間で暗号通信を行う際に用いる暗号鍵の更新方法であって、前記暗号通信を行う通信装置において複数の暗号鍵と各暗号鍵を特定する識別子から構成された暗号鍵テーブルを作成し、暗号通信を行う前記通信装置のうちの第１の通信装置が前記暗号鍵テーブルから識別子を選択し、その識別子を暗号鍵により暗号化して前記暗号通信を行う通信装置のうちの第２の通信装置にへ通知し、通知された前記第２の通信装置が暗号鍵により暗号化された識別子を復号し、前記第１の通信装置および識別子を復号した前記第２の通信装置が、識別子に対応する暗号鍵を前記暗号鍵テーブルから取り出し、該暗号鍵を用いて前記第１、第２の通信装置間で暗号通信を行うものである。

【００３３】また、その他の解決手段は、複数の通信装置がネットワークで接続され、前記複数の通信装置の間で暗号通信を行う際に用いる暗号鍵の更新方法であって、前記暗号通信を行う通信装置はそれぞれ同一のマスタ鍵を保持し、暗号通信を行う前記通信装置のうち第１の通信装置がハッシュ鍵を生成し、前記ハッシュ鍵を暗化鍵で暗号化し、暗号化された前記ハッシュ鍵を前記暗号通信を行う通信装置のうちの第２の通信装置へ通知し、前記ハッシュ鍵が通知された前記第２の通信装置が暗号鍵で該暗号化されたハッシュ鍵を復号し、前記第１、第２の通信装置がマスタ鍵をハッシュ鍵によってハッシュした結果を暗号鍵として前記第１、第２の通信装置間で暗号通信を行うものである。

【００３４】さらに、その他の解決手段は、複数の通信装置がネットワークで接続され、前記複数の通信装置の間で暗号通信を行う際に用いる暗号鍵の更新方法であって、前記暗号通信を行う通信装置において複数の暗号鍵と各暗号鍵を特定する識別子から構成された暗号鍵マスタテーブルを作成し、前記暗号通信を行う通信装置のうちの第１の通信装置が前記暗号鍵マスタテーブルから任意の識別子を選択し、その識別子を暗号鍵で暗号化して前記暗号通信を行う通信装置のうちの第２の通信装置へ通知し、前記第１の通信装置がハッシュ鍵を生成し、前記ハッシュ鍵を該暗号鍵により暗号化して前記第２の通信装置に通知し、暗号化された識別子が通知された前記第２の通信装置が、暗号化された識別子および前記ハッシュ鍵を復号し、識別子に対応する暗号鍵を前記暗号鍵マスタテーブルから取り出し、暗号鍵を前記ハッシュ鍵によってハッシュした結果を暗号鍵とし、その暗号鍵を用いて前記第１、第２の通信装置間で暗号通信を行うものである。

【００３５】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。

【００３６】（実施の形態１）図１は、本発明の実施の形態１による通信装置におけるネットワーク構成の説明図、図２は、本発明の実施の形態１による通信装置におけるブロック図、図３、図４は、本発明の実施の形態１による暗号鍵変更処理の説明図、図５は、本発明の実施の形態１による暗号鍵テーブルの構成図、図６、図７は、本発明の実施の形態１による暗号鍵変更のフローチャートである。

【００３７】本実施の形態において、暗号通信を行うネットワーク構成は、図１に示すように、たとえば、パーソナルコンピュータなどの暗号通信を行う通信装置１～３が、それぞれネットワーク４に接続されている。また、この場合、通信装置１と通信装置２の間および通信装置１と通信装置３の間でそれぞれ独立に暗号通信が行われるものとする。

【００３８】次に、通信装置１における構成を図２を用いて説明する。

【００３９】まず、通信装置１は、フロッピーディスクドライブ５、ハードディスクドライブ６、ＣＤ－ＲＯＭドライブ７、通信コントローラ8_1～8_n、メインメモリ９、通信装置１のすべての制御を司るＣＰＵ１０ならびにバスの制御を行うバスコントローラ１１により構成され、これらは内部バス１２により接続されている。

【００４０】そして、通信プログラムと後述する暗号鍵テーブルは、フロッピーディスクドライブ５またはＣＤ－ＲＯＭドライブ７からハードディスクへインストールするか直接メインメモリ９へローディングを行う。また、ハードディスクにインストールした場合は、ハードディスクからメインメモリ９へローディングを行うものとする。さらに、フロッピーディスクドライブ５またはＣＤ－ＲＯＭドライブ７からネットワーク４を介して他の通信装置へインストールすることもできる。

【００４１】なお、暗号鍵テーブルは、暗号鍵テーブル

の形式でフロッピーディスクドライブ５またはＣＤ－ＲＯＭドライブ７に格納されてもよいし、他のデータから暗号鍵テーブル生成プログラムにより生成されてもよい。

【００４２】次に、通信コントローラ8_1～8_nは、物理レベル（ＭＡＣ層以下）制御のみを行うものとし、メインメモリ９に設けられた送受信バッファ９ａとのデータ転送は通信コントローラ8_1～8_nに設けられたダイレクトメモリアクセス（ＤＭＡ）によって行う。また、通信コントローラ8_1～8_n内にＣＰＵ１０を設けて、そこで通信プログラムを動作させることや通信コントローラ8_1～8_n内に送受信二次バッファを設け、ＣＰＵ１０がメインメモリ９上の送受信バッファ９ａとの間でデータ転送することも可能である。また、図２においては、通信装置１における回路構成について説明したが、その他の通信装置２，３も同様の構成とする。

【００４３】次に、それぞれの通信装置における暗号鍵の設定について説明する。

【００４４】まず、図３に示すように、それぞれの通信装置１～３に暗号通信を行う相手毎に複数の暗号鍵を登録してある後述する暗号鍵テーブルを設定する。すなわち、通信装置１には、通信装置２および通信装置３のそれぞれと暗号通信するために用いる暗号鍵テーブルＴａｂとＴａｃを設定する。

【００４５】また、通信装置２には、通信装置１と暗号通信を行うための暗号鍵テーブルＴａｂを設定を行い、通信装置３には、通信装置１と暗号通信を行うための暗号鍵テーブルＴａｃの設定を行う。

【００４６】ここで、通信装置１の暗号鍵テーブルＴａｂと通信装置２の暗号鍵テーブルＴａｂおよび通信装置１暗号鍵テーブルＴａｃと通信装置３の暗号鍵テーブルＴａｃはそれぞれ同一のものである。さらに、これらは、複数の暗号鍵とそれぞれの鍵に対応した任意の識別子であるＩＤから構成されている。

【００４７】そして、このＩＤを用いて暗号鍵テーブルの中からどの鍵を使用するかを指定を行う。たとえば、通信装置１と通信装置２の間の暗号通信でＩＤ＝５の鍵を用いる場合には、それぞれの通信装置１，２に初期値としてＩＤ＝５を設定する。同様に、通信装置１と通信装置３の間の暗号通信でＩＤ＝３の鍵を用いる場合には、それぞれの通信装置１，３に初期値としてＩＤ＝３を設定する。

【００４８】次に、それぞれの通信装置１～３では、設定されたＩＤに基づいてそれぞれの暗号鍵テーブルから一つの暗号鍵を取り出し、送信するデータの暗号および受信したデータの復号に用いて暗号通信を行う。

【００４９】たとえば、ＩＤ＝ｎの暗号鍵をＫ［ＩＤ＝ｎ］と表現すると、通信装置１と通信装置２間および通信装置１と通信装置２間の暗号通信でそれぞれ使用する暗号鍵は、それぞれ暗号鍵Ｋａｂ［ＩＤ＝５］および暗号鍵Ｋａｃ［ＩＤ＝３］となる。

【００５０】ここで、通信装置１と通信装置２の間の暗号通信の暗号鍵を変更する場合について図４を用いて説明する。

【００５１】まず、通信装置１で暗号鍵のＩＤを、たとえば、ＩＤ＝８に変更する。通信装置１では、暗号鍵テーブルＴａｂからＩＤ＝８に相当する暗号鍵Ｋａｂ［ＩＤ＝８］を取り出す。

【００５２】これと同時に通信装置１から通信装置２へＩＤ変更コマンドＨＣとしてＩＤ＝８を送信する。通信装置２では、該ＩＤ変更コマンドＨＣからＩＤ＝８を取り出し、暗号鍵テーブルＴａｂからＩＤ＝８に相当する暗号鍵Ｋａｂ［ＩＤ＝８］を取り出す。

【００５３】これによって、通信装置１と通信装置２の暗号化鍵が変更できるので、通信装置１と通信装置２間の暗号通信は変更した暗号鍵Ｋａｂ［ＩＤ＝８］を用いて続けることが可能となる。

【００５４】なお、暗号鍵テーブルは暗号化して保持しておくことが望ましい。また、ＩＤ変更コマンドＨＣは、暗号化して送信することが望ましい。さらに、ＩＤ変更コマンドＨＣを暗号化するときの暗号鍵は、変更前の暗号化鍵であることが望ましい。また、通信装置１と通信装置２の暗号鍵テーブルＴａｂと通信装置１と通信装置３のＴａｃは同一であってもよい。

【００５５】すなわち、複数のまたはすべての通信装置１～３間での暗号通信において同一の暗号鍵テーブルを使用してもよい。その場合、通信装置１には設定する同じ暗号鍵テーブルは一つであってよく、ＩＤも複数の通信装置間で同一のＩＤを用いてもよい。

【００５６】また、変更するＩＤは、通信装置の管理者が指定してもよいし、通信装置１～３内の乱数によって選択してもよい。

【００５７】次に、暗号鍵テーブルＴａｂ（図３）の構成を図５に示す。

【００５８】暗号鍵テーブルＴａｂは、複数の暗号鍵Ｋａｂを保持する領域とそれに対応した識別子であるＩＤを保持する領域から構成される。

【００５９】通信装置１での処理手順について図３～図５および図６に示す処理フローを用いて説明する。

【００６０】まず、ＣＰＵ１０が初期設定によって暗号鍵テーブルＴａｂとＩＤ＝５の設定を行い（ステップＳ１０１）、暗号鍵テーブルＴａｂからＩＤ＝５に相当する暗号鍵Ｋｚ を選択する（ステップＳ１０２）。

【００６１】次に、ＣＰＵ１０は、送信カウンタをゼロに設定し（ステップＳ１０３）、暗号通信を開始する（ステップＳ１０４）。そして、ＣＰＵ１０は、通信装置２宛のパケットを暗号鍵Ｋｚ で暗号化してネットワーク４に送信し（ステップＳ１０５）、送信カウンタを１インクリメントする（ステップＳ１０６）。

【００６２】その時、送信カウンタが１００未満の場合

にはステップＳ１０５の処理に戻り、通信装置２宛の暗号通信を繰り返す。

【００６３】また、ＣＰＵ１０は、送信カウンタが１００以上の場合、ＩＤの更新処理へ移行する（ステップＳ１０７）。ＣＰＵ１０は、新しいＩＤ＝８を乱数によって選択し（ステップＳ１０８）、そのＩＤ＝８を暗号鍵Kx で暗号化したデータKx［ＩＤ＝８］をＩＤ変更コマンドＨＣに付加して通信装置２宛にネットワーク４に対して送信する（ステップＳ１０９）。

【００６４】そして、ステップＳ１０２の処理に戻り、暗号鍵テーブルTabからＩＤ＝８に対応する暗号鍵Kuを取り出す。その後、送信カウンタをゼロに再設定し、以降送信カウンタが１００以上になるまで暗号鍵Ku を用いて通信装置２宛のパケットを暗号化して送信を行う。

【００６５】次に、通信装置２での処理手順について図３～図５ならびに図７を用いて説明する。

【００６６】まず、ＣＰＵ１０が初期設定によって暗号鍵テーブルTabとＩＤ＝５を設定した後（ステップ２０１）、暗号鍵テーブルTabからＩＤ＝５に相当する暗号鍵Kz を選択する（ステップＳ２０２）。

【００６７】次に、通信装置１から受信したパケットを送受信バッファ９ａに書き込み、ＣＰＵ１０が暗号鍵Ｋz を用いて復号する（ステップＳ２０３）。ＣＰＵ１０は復号したパケットがＩＤ変更コマンドＨＣか否かを判別する（ステップＳ２０４）。

【００６８】そして、該パケットがＩＤ変更コマンドＨＣでない場合は、ＣＰＵ１０が該パケットに適応した受信処理（たとえば、アプリケーションにデータを引き渡すなど）を行い（ステップＳ２０５）、ステップＳ２０３の処理に戻る。一方、該パケットがＩＤ変更コマンド３３である場合、ＣＰＵ１０は該パケットから変更されたＩＤ＝８を取り出す（ステップＳ２０６）。

【００６９】そして、ステップＳ２０２の処理に戻り、暗号鍵テーブルTabのＩＤ＝８に対応する暗号鍵Ku を取り出す。以降、新たなＩＤ変更コマンドを受信するまでまで暗号鍵Ku を用いて通信装置１から受信したパケットを復号化する。

【００７０】以上のようにして通信装置１からＩＤ変更コマンドＨＣが発信されるまでは、通信装置１と通信装置２間では、暗号鍵Kz を用い、通信装置２でＩＤ変更コマンドＨＣが受信された後は、通信装置１と通信装置２間では、暗号鍵Ku を用いて暗号通信を行うことができる。

【００７１】従って通信装置管理者は、初期設定情報として通信装置１と通信装置２にそれぞれ暗号鍵テーブルTabとＩＤ＝５を設定するだけで、あとは自動的に鍵が更新される。

【００７２】また、本実施の形態では、送信カウンタの判定値を１００に設定したが、該判定値は管理者が自由に設定してよい。また、暗号鍵テーブルTabは、管理者以外がアクセスできない領域に保持することが望ましく、暗号鍵テーブルTab自体を別の暗号鍵で暗号化して保持しておくことが望ましい。

【００７３】ここで、通常暗号文を解読するためには、膨大な時間と計算機パワーを必要とする。ただし、偶然にも暗号鍵を見つけだすことは不可能とは言い切れない。したがって、第三者が偶然暗号鍵を手に入れた場合、その暗号鍵を使っている以上、暗号文はすべて第三者に解読可能になってしまう。

【００７４】そこで、本実施の形態１においては、暗号鍵を定期的に変更することによって上記問題点による弊害を最小限にするようにしている。

【００７５】すなわち、前述したように第三者が偶然にも暗号鍵を手に入れると、第三者はその暗号鍵を使って暗号文を解読することが可能となる。しかし、暗号鍵は定期的に変更しているので第三者は、暗号文を解読できなくなる。

【００７６】このように、暗号文が解読されるのはごく一次的なものであり、データすべてが解読されることはない。さらに、暗号鍵の変更間隔を短くすることによって、解読されるデータを最小限に押さえることができる。

【００７７】（実施の形態２）図８、図９は、本発明の実施の形態２による暗号鍵変更処理の説明図、図１０、図１１は、本発明の実施の形態２による暗号鍵変更のフローチャートである。

【００７８】本実施の形態２においては、前述した図１、図２と同じシステム構成におけるそれぞれの通信装置１～３に暗号鍵を設定する手順を図８を用いて説明する。

【００７９】まず、それぞれの通信装置１～３に暗号通信を行う相手毎にマスタ鍵ＭＫとマスタ鍵ＭＫにハッシュをかけて暗号鍵を生成するためのハッシュ鍵ＨＫを設定する。

【００８０】すなわち、通信装置１には、通信装置２および通信装置３とそれぞれ暗号通信を行う時に使う暗号鍵を生成するためのマスタ鍵MKab，MKacとハッシュ鍵ＨKab，ＨKacを設定する。

【００８１】また、通信装置２には、通信装置１と暗号通信を用いる時に使用する暗号鍵を生成するためのマスタ鍵MKabとハッシュ鍵ＨKabを設定する。なお、通信装置１のマスタ鍵MKabと通信装置２のマスタ鍵MKabおよび通信装置１のハッシュ鍵ＨKabと通信装置２のハッシュ鍵ＨKabはそれぞれ同一である。

【００８２】同様に、通信装置３にも、通信装置１と暗号通信を行う時に使う暗号鍵を生成するためのマスタ鍵MKacとハッシュ鍵ＨKacを設定する。なお、通信装置１のマスタ鍵MKacと通信装置３のマスタ鍵MKacおよび通信装置１のハッシュ鍵ＨKacと通信装置３のハッシ

ュ鍵ＨＫacはそれぞれ同一である。

【００８３】それぞれの通信装置１～３では、マスタ鍵ＭＫとハッシュ鍵ＨＫから暗号化鍵Ｋ＝ＨＫ（ＭＫ）を生成する。通信装置１と通信装置２間で暗号通信を行うために、通信装置１と通信装置２では、それぞれ暗号鍵ＨＫab（ＭＫab）を生成する。また、通信装置１と通信装置２間では、該暗号鍵ＨＫＫab（ＭＫab）を用いて暗号通信を行う。

【００８４】ここで、暗号鍵を変更する手順を図９を用いて説明する。

【００８５】まず、通信装置１においてハッシュ鍵を変更する。変更方法は、通信装置１の管理者が行ってもよいし、通信装置内の乱数から求めてもよい。

【００８６】通信装置１のハッシュ鍵がハッシュ鍵ＨＫ’abに変更されると、通信装置１では、暗号化鍵Ｋ＝ＨＫ’ab（ＭＫab）が生成される。同時に、通信装置１は、変更されたハッシュ鍵ＨＫ’abをハッシュ鍵変更コマンドＨＨＣによって通信装置２に送信する。そのハッシュ鍵変更コマンドＨＨＣを受信した通信装置２は、該ハッシュ鍵変更コマンドＨＨＣからハッシュ鍵ＨＫ’abを取り出し、該ハッシュ鍵ＨＫ’abを用いて暗号鍵ＨＫ’ab（ＭＫab）を生成する。

【００８７】以降、通信装置１と通信装置２間で暗号鍵ＨＫ’ab（ＭＫab）を用いて暗号通信が行われる。なお、マスタ鍵とハッシュ鍵は暗号化して保持しておくこと望ましく、ハッシュ鍵変更コマンドＨＨＣも暗号化して送信することが望ましい。

【００８８】また、ハッシュ鍵変更コマンドＨＨＣを暗号化するときの暗号化鍵は、変更前の暗号鍵を使うことが望ましい。さらに、マスタ鍵、ハッシュ鍵またはマスタ鍵とハッシュ鍵の両方は、複数またはすべての通信装置で同一でもよい。その場合、同一のマスタ鍵または同一のハッシュ鍵を一つの通信装置内で通信相手毎に保持せずに共通に使用してもよい。

【００８９】次に、通信装置１での処理手順について図８、図９および図１０に示す処理フローを用いて説明する。

【００９０】まず、ＣＰＵ１０が初期設定によってマスタ鍵ＭＫabとハッシュ鍵ＨＫabを設定し（ステップＳ３０１）、送信タイマをゼロにセットする（ステップＳ３０２）。なお、該送信タイマは、別タスクにて自動的に更新されているか、ハードウェアで自動更新されているものとする。

【００９１】そして、ＣＰＵ１０はマスタ鍵をハッシュ鍵でハッシュした結果（＝ＨＫab（ＭＫab））を暗号鍵Ｋに設定を行い（ステップＳ３０３）、暗号通信を開始する（ステップＳ３０４）。

【００９２】通信装置２宛のパケットを暗号鍵Ｋで暗号化してネットワーク４に送信する（ステップＳ３０５）。その後、送信タイマを読み込み（ステップＳ３０６）、送信タイマが５分を越えているか否かの判定を行う（ステップＳ３０７）。

【００９３】ここで、該送信タイマが５分以内の場合には、ステップＳ３０４の処理に戻り、通信装置２宛の次のパケットを暗号鍵Ｋで暗号化してネットワーク４に対して送信する。

【００９４】一方、該送信タイマが５分を越えていた場合には、内部の乱数により新しいハッシュ鍵ＨＫ’abを生成し（ステップＳ３０８）、新しいハッシュ鍵ＨＫ’abを暗号鍵Ｋで暗号化して、該暗号化したデータをハッシュ鍵変更コマンド４７に付加し、通信装置２宛てネットワーク４に対して送信を行い（ステップＳ３０９）、ステップＳ３０２に戻って再び送信タイマをゼロにセットする。

【００９５】その後、マスタ鍵ＭＫabを新しいハッシュ鍵ＨＫ’abでハッシュした結果（＝ＨＫ’ab（ＭＫab））を新しい暗号鍵Ｋに設定する。以降、送信タイマ値が５分を越えるまで新しい暗号鍵Ｋを用いて通信装置２宛のパケットを暗号化して、該暗号化したパケットをネットワーク４に対して送信する。

【００９６】次に、通信装置２での処理手順について図８、図９ならびに図１１を用いて説明する。

【００９７】まず、ＣＰＵ１０が初期設定によってマスタ鍵ＭＫabとハッシュ鍵ＨＫabの設定を行う（ステップＳ４０１）。そして、ＣＰＵ１０がマスタ鍵をハッシュ鍵でハッシュした結果（＝ＨＫab（ＭＫab））を暗号鍵Ｋに設定する（ステップＳ４０２）。

【００９８】通信装置１から送信されたパケットをネットワーク４から受信すると、該パケットを送受信バッファ９ａに書き込み、ＣＰＵ１０が暗号鍵Ｋで復号化する（ステップＳ４０３）。ＣＰＵ１０が該復号したパケットがハッシュ鍵変更コマンドＨＨＣであるか否かを判定する（ステップＳ４０４）。

【００９９】そして、ＣＰＵ１０は、ハッシュ鍵変更コマンドＨＨＣでない場合、該パケットに適応した受信処理（たとえば、アプリケーションにデータを引き渡すなど）を行い（ステップＳ４０５）、ステップＳ４０３の処理に戻る。

【０１００】一方、該パケットがハッシュ鍵変更コマンドＨＨＣである場合、ＣＰＵ１０は該パケットから変更されたハッシュ鍵ＨＫ’abを取り出す（ステップＳ４０６）。そして、ステップＳ４０２の処理に戻り、マスタ鍵ＭＫabを上記取り出した新しいハッシュ鍵ＨＫ’abでハッシュした結果（＝ＨＫ’ab（ＭＫab））を新しい暗号鍵Ｋとして設定する。以降、新たなハッシュ鍵変更コマンドを受信するまで暗号鍵Ｋを用いて通信装置１から受信したパケットを復号化する。

【０１０１】以上のようにして通信装置１からハッシュ鍵変更コマンドＨＨＣが発信されるまでは、通信装置１と通信装置２間では、暗号鍵Ｋ（＝ＨＫab（ＭＫab））

を用い、通信装置２でハッシュ鍵変更コマンドＨＨＣが受信された後は、通信装置１と通信装置２間では、暗号鍵Ｋ（＝ＨＫ’ab（ＭＫab））を用いて暗号通信を行うことができる。

【０１０２】したがって、通信装置管理者が、初期設定情報として通信装置１と通信装置２にそれぞれマスタ鍵ＭＫabとハッシュ鍵ＨＫabを設定するだけで、自動的に鍵の更新が行われることになる。

【０１０３】なお、本実施の形態２においては、送信タイマの判定値を５分に設定したが、該判定値は管理者が自由に設定してよい。また、マスタ鍵ＭＫabとハッシュ鍵ＨＫabは、管理者以外がアクセスできない領域に保持することが望ましい。さらにマスタ鍵ＭＫabとハッシュ鍵ＨＫab自体を別の暗号鍵で暗号化して保持しておくことが望ましい。

【０１０４】また、本実施の形態２でも、暗号鍵を定期的に変更することによって暗号文の解読をごく一次的なものとし、データすべてが解読されることを防止することができる。さらに、暗号鍵の変更間隔を短くすることによって、解読されるデータを最小限に押さえることができる。

【０１０５】（実施の形態３）図１２、図１３は、本発明の実施の形態３による暗号鍵変更処理の説明図、図１４は、本発明の実施の形態３による暗号鍵マスタテーブル、図１５、図１６は、本発明の実施の形態３による暗号鍵変更のフローチャートである。

【０１０６】本実施の形態３では、前述した図１、図２と同じシステム構成におけるそれぞれの通信装置１～３に暗号鍵を設定する手順を図１２を用いて説明する。

【０１０７】それぞれの通信装置１～３には、同一の暗号鍵マスタテーブルＭＴを設定する。該暗号マスタテーブル鍵ＭＴは、複数の暗号鍵（ＭＫ［ＩＤ］）とそれに対応するＩＤで構成される。

【０１０８】実際に暗号通信を行う時の暗号鍵Ｋは、複数の暗号鍵ＭＫ［ＩＤ］をハッシュ鍵ＨＫでハッシュしたＫ＝ＨＫ（ＭＫ［ＩＤ］）により生成する。ここで、通信装置１と通信装置２間での暗号通信のための暗号鍵を生成するためのＩＤとハッシュ鍵を通信装置１と通信装置２に、それぞれＩＤ＝６、ＨＫabと設定すると通信装置１と通信装置２ではそれぞれ暗号鍵Ｋ＝ＨＫab（ＭＫ［６］）を生成する。

【０１０９】そして、該暗号鍵Ｋを用いて暗号通信を行う。同様に通信装置１と通信装置３間での暗号通信のための暗号鍵を生成するためのＩＤとハッシュ鍵を通信装置１と通信装置２にそれぞれＩＤ＝８、ＨＫacとすると通信装置１と通信装置２では、それぞれ暗号鍵Ｋ＝ＨＫac（ＭＫ［８］）を生成する。そして該暗号鍵Ｋを用いて暗号通信を行う。

【０１１０】次に通信装置１と通信装置２間の暗号鍵を変更する手順を図１３を用いて説明する。

【０１１１】まず、通信装置１のＩＤとハッシュ鍵をそれぞれＩＤ＝５とハッシュ鍵ＨＫ’abに変更する。通信装置１では、暗号鍵Ｋ＝ＨＫ’ab（ＭＫ［５］）を生成する。

【０１１２】これと同時に、通信装置１は変更されたＩＤ＝５とハッシュ鍵ＨＫ’abを鍵変更コマンドＫＨＣによって通信装置２に通知する。該鍵変更コマンドＫＨＣを受信した通信装置２は、該鍵変更コマンドＫＨＣからＩＤ＝５とハッシュ鍵ＨＫ’abを取り出し、暗号鍵Ｋ＝ＨＫ’ab（ＭＫ［５］）を生成する。通信装置１と通信装置２間では、該新しい暗号鍵Ｋを用いて暗号通信を行う。

【０１１３】なお、暗号鍵マスタテーブルは、暗号化して保持しておくことが望ましい。鍵変更コマンドは暗号化して送信することが望ましい。鍵変更コマンドを暗号化するときの暗号鍵は、変更する前の暗号鍵であることが望ましい。暗号鍵マスタテーブルは、システムで同一としたが、通信相手毎に別テーブルを用いてもよい。ＩＤとハッシュ鍵は通信相手毎の固有の値にしたが、ＩＤ、ハッシュ鍵または、両方をシステムで共通にしてもよい。

【０１１４】次に、暗号鍵マスタテーブルＭＴの構成を図１４に示す。

【０１１５】暗号鍵マスタテーブルＭＴは、複数の暗号鍵Ｋを保持する領域とそれに対応した識別子ＩＤを保持する領域から構成される。

【０１１６】ここで、通信装置１での処理手順について図１２～図１４ならびに図１５に示す処理フローを用いて説明する。

【０１１７】まず、ＣＰＵ１０が初期設定によって暗号鍵マスタテーブルＭＴ、ＩＤ＝６とハッシュ鍵ＨＫabを設定する（ステップＳ５０１）。次に、ＣＰＵ１０は、暗号鍵マスタテーブルＭＴからＩＤ＝６に相当する暗号マスタ鍵Ｋw を選択し、該マスタ暗号鍵Ｋw をハッシュ鍵ＨＫabでハッシュした結果（＝ＨＫab（Ｋw））を暗号鍵Ｋとして設定し（ステップＳ５０２）、暗号通信を開始する（ステップＳ５０３）。

【０１１８】そして、ＣＰＵ１０は、通信装置２宛のパケットを暗号鍵Ｋで暗号化してネットワーク４（図１）に送信して（ステップＳ５０４）、暗号鍵変更要求があるか否かの判定を行う（ステップＳ５０５）。

【０１１９】ここで、該暗号鍵変更要求とは、管理者が暗号鍵の変更を行うために、管理者インタフェースを用いて暗号鍵の変更（具体的には新しいＩＤとハッシュ鍵の設定）を指示する事であり、該指示により通信装置のプログラムが読み込み可能な鍵変更要求フラグがセットされる。また、通信装置のプログラムは該鍵変更要求フラグがセットされたことによって暗号鍵変更要求があると判断する。

【０１２０】次に、管理者が暗号鍵の変更要求を実行し

ていない場合には、該暗号鍵変更要求フラグがセットされていないので再びステップＳ５０４の処理に戻り、引き続き暗号鍵Ｋで通信装置２宛のパケットを暗号化して、該パケットをネットワーク４に対して送信する。

【０１２１】一方、管理者が所定の入力手段によって暗号鍵の変更要求を実行した場合には、ＣＰＵ１０によってメインメモリ９上に暗号鍵変更要求フラグが設定され、新しく設定されたＩＤ＝５とハッシュ鍵ＨＫ’abを読み込み、該暗号鍵変更要求フラグをリセットする（ステップＳ５０６）。

【０１２２】ＣＰＵ１０は、該読み込んだＩＤ＝５とハッシュ鍵ＨＫ’abを暗号鍵Ｋで暗号化したデータを鍵変更コマンドＫＨＣに付加して通信装置２宛にネットワーク４に対して送信する（ステップＳ５０７）。

【０１２３】ステップＳ５０２の処理に戻り、暗号鍵マスタテーブルＭＴからＩＤ＝５に対応する暗号鍵Ky を取り出す。そして、暗号鍵変更要求フラグがセットされるまで暗号鍵Ky を用いて通信装置２宛のパケットを暗号化して送信する。

【０１２４】次に、通信装置２での処理手順について図１２～図１４および図１７を用いて説明する。

【０１２５】まず、ＣＰＵ１０は、初期設定によって暗号鍵マスタテーブルＭＴ、ＩＤ＝６とハッシュ鍵ＨＫabを設定する（ステップＳ６０１）。ＣＰＵ１０は、暗号鍵マスタテーブルＭＴからＩＤ＝６に相当する暗号マスタ鍵Kw を選択し、該マスタ暗号鍵Kw をハッシュ鍵ＨＫabでハッシュした結果（＝ＨＫab（Ｋｗ））を暗号鍵Ｋとして設定する（ステップＳ６０２）。

【０１２６】そして、ＣＰＵ１０は、通信装置１から受信したパケットを暗号鍵Kw を用いて復号を行う（ステップＳ６０３）。該復号したパケットが鍵変更コマンドＫＨＣか否かをＣＰＵ１０が判別し（ステップＳ６０４）、該パケットが鍵変更コマンドＫＨＣでない場合、ＣＰＵ１０は該パケットに適応した受信処理（たとえば、アプリケーションにデータを引き渡すなど）を行い（ステップＳ６０５）、ステップＳ６０３の処理に戻る。

【０１２７】一方、該パケットが鍵変更コマンドＫＨＣである場合は、ＣＰＵ１０が該パケットから変更されたＩＤ＝５とハッシュ鍵ＨＫ’abを取り出す（ステップＳ６０６）。

【０１２８】そして、ステップＳ６０２に戻り、暗号鍵マスタテーブルＭＴのＩＤ＝５に対応する暗号鍵Ky を取り出す。以降、新たな鍵変更コマンドを受信するまで暗号鍵Ky を用いて通信装置１から受信したパケットを復号化する。

【０１２９】以上のようにして通信装置１から鍵変更コマンドＫＨＣが発信されるまでは、通信装置１と通信装置２間では、暗号鍵Kw を用い、通信装置２で鍵変更コマンドＫＨＣが受信された後は、通信装置１と通信装置２間では、暗号鍵Ky を用いて暗号通信を行うことができる。

【０１３０】したがって、通信装置管理者は、初期設定情報として通信装置１と通信装置２にそれぞれ暗号鍵マスタテーブルＭＴとＩＤ＝６を設定し、鍵を変更したいときに必要な情報を一つの通信装置に設定するだけで、あとは自動的に鍵の更新が行われることになる。

【０１３１】なお、暗号鍵マスタテーブルＭＴ、ＩＤおよびハッシュ鍵は、管理者以外がアクセスできない領域に保持することが望ましい。さらに、暗号鍵マスタテーブルＭＴ、ＩＤおよびハッシュ鍵はそれ自体を別の暗号鍵で暗号化して保持しておくことが望ましい。

【０１３２】また、本実施の形態３によっても、暗号鍵を定期的に変更することによって暗号文の解読をごく一次的なものとし、データすべてが解読されることを防止することができる。さらに、暗号鍵の変更間隔を短くすることによって、解読されるデータを最小限に押さえることができる。

【０１３３】本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【０１３４】たとえば、前記実施の形態１～３では、相互の通信装置間において、個別のテーブルを用いた暗号鍵の更新技術について記載したが、３つ以上の複数の通信装置が共通のテーブル用いて暗号鍵の更新を行うようにしてもよい。

【０１３５】また、前記実施の形態１～３においては、データの暗号化および暗号化されたデータの複号の処理は、ソフトウェアあるいはハードウェアの何れによって実現されてもよい。

【０１３６】

【発明の効果】

（１）本発明によれば、暗号鍵の変更をすべての通信装置に対して行わなくてよいので、管理者の負担を大幅に軽減でき、かつ暗号鍵の設定ミスも防止することができる。

【０１３７】（２）また、本発明では、暗号鍵更新時に通信装置間においてやり取りされるデータが暗号鍵それ自体ではないので、セキュリティを大幅に向上させることができる。

【０１３８】（３）さらに、本発明においては、暗号鍵の更新時における通信装置を一時的に停止させなくてよいので、作業効率をより向上することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態１による通信装置におけるネットワーク構成の説明図である。

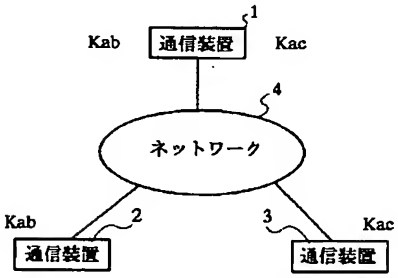
【図２】本発明の実施の形態１による通信装置におけるブロック図である。

【図３】本発明の実施の形態１による暗号鍵変更処理の説明図である。

【図４】本発明の実施の形態１による暗号鍵変更処理の説明図である。
【図５】本発明の実施の形態１による暗号鍵テーブルの構成図である。
【図６】本発明の実施の形態１による暗号鍵変更のフローチャートである。
【図７】本発明の実施の形態１による暗号鍵変更のフローチャートである。
【図８】本発明の実施の形態２による暗号鍵変更処理の説明図である。
【図９】本発明の実施の形態２による暗号鍵変更処理の説明図である。
【図１０】本発明の実施の形態２による暗号鍵変更のフローチャートである。
【図１１】本発明の実施の形態２による暗号鍵変更のフローチャートである。
【図１２】本発明の実施の形態３による暗号鍵変更処理の説明図である。
【図１３】本発明の実施の形態３による暗号鍵変更処理の説明図である。
【図１４】本発明の実施の形態３による暗号鍵マスタテーブルである。
【図１５】本発明の実施の形態３による暗号鍵変更のフローチャートである。
【図１６】本発明の実施の形態３による暗号鍵変更のフローチャートである。
【図１７】本発明者が検討した暗号鍵変更処理の説明図である。
【図１８】本発明者が検討した暗号鍵変更処理におけるシーケンス図である。
【符号の説明】
１～３…通信装置，４…ネットワーク，５…フロッピーディスクドライブ，６…ハードディスクドライブ，７…ＣＤ－ＲＯＭドライブ，8_1～8_n…通信コントローラ，９…メインメモリ，９ａ…送受信バッファ，１０…ＣＰＵ，１１…バスコントローラ，１２…内部バス，Ｔab、Ｔac…暗号鍵テーブル，Ｋab、Ｋac…暗号鍵，ＨＣ…ＩＤ変更コマンド，ＭＫ…マスタ鍵…，ＨＫ…ハッシュ鍵，ＨＨＣ…ハッシュ鍵変更コマンド，ＭＴ…暗号鍵マスタテーブル，ＫＨＣ…鍵変更コマンド。

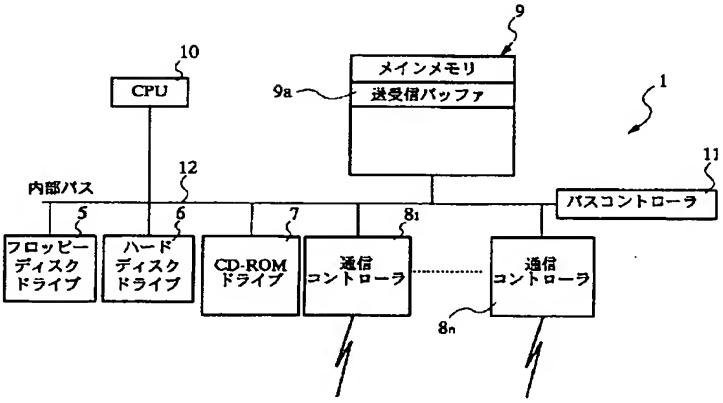
【図１】

図 1



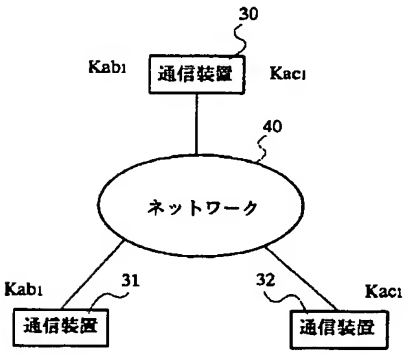
【図２】

図 2



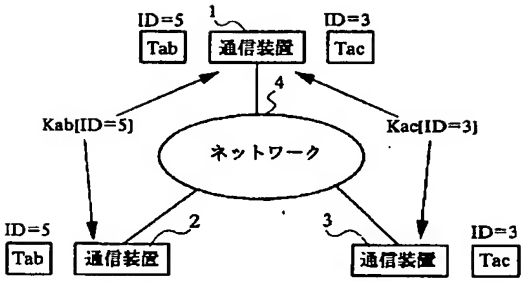
【図１７】

図 17



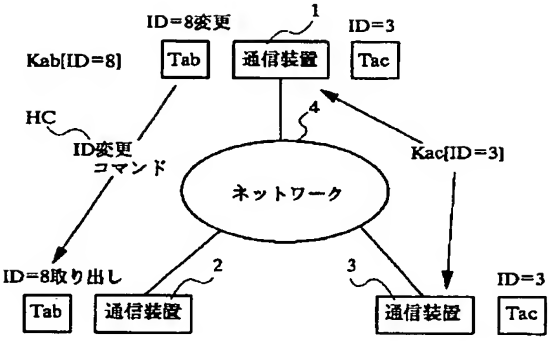
【図３】

図　3



【図４】

図　4



【図５】

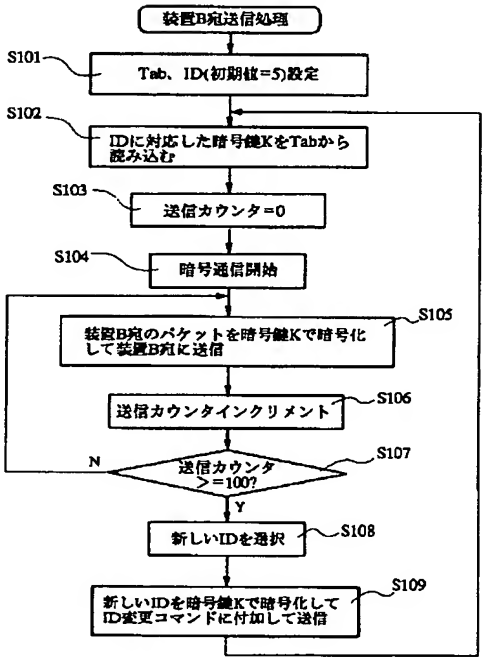
図　5

ID	Kab
3	Kx
5	Kz
10	Ky
7	Kv
⋮	⋮
8	Ku

Tab

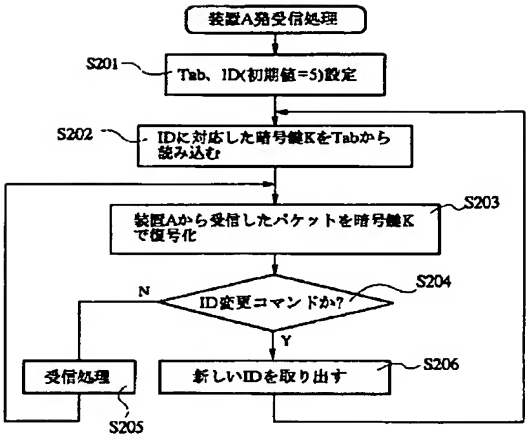
【図６】

図　6



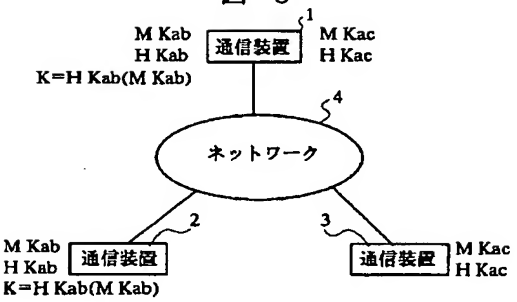
【図７】

図 7



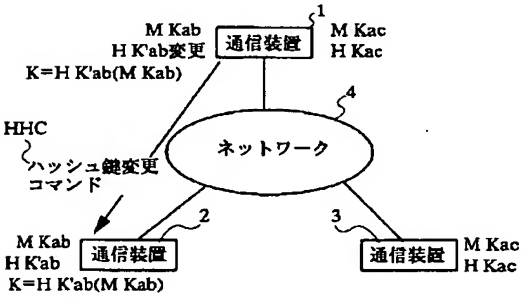
【図８】

図 8



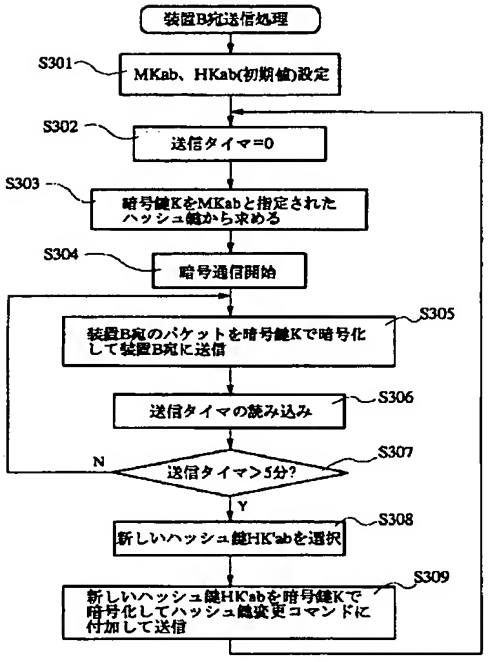
【図９】

図 9



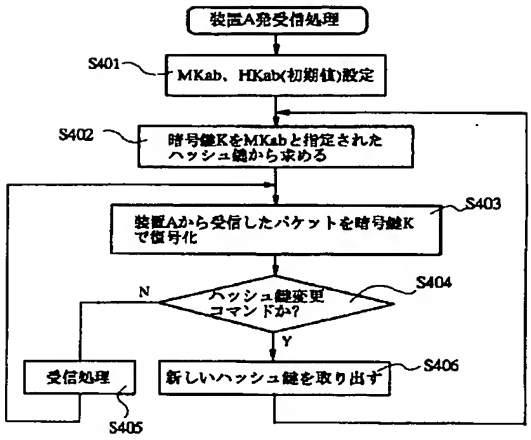
【図１０】

図 10



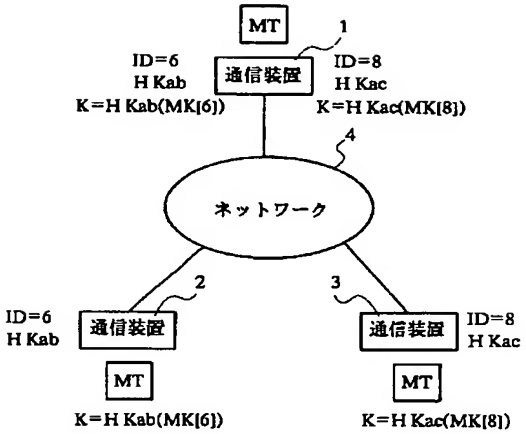
【図１１】

図 11



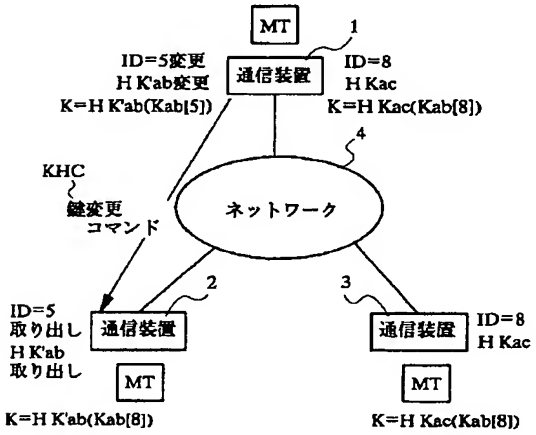
【図１２】

図 12



【図１３】

図 13



【図１４】

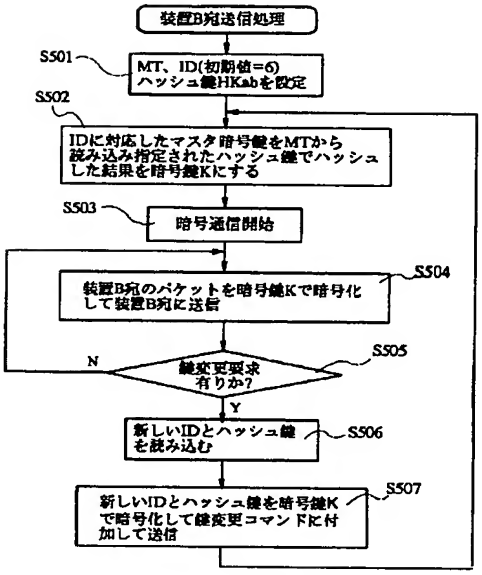
図 14

ID	Kab
3	Kz
5	Ky
10	Kx
6	Kw
⋮	⋮
8	Kv

MT

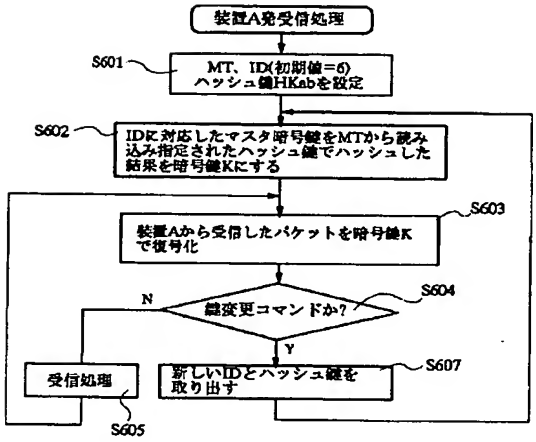
【図１５】

図　15



【図１６】

図　16



【図１８】

図　18